Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшаего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.04 Программная инженерия (Технологии больших данных)
Отделение информационных технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях

УДК 004.415:004.774.056.523

Студент

Группа	ФИО	Подпись	Дата
8ПМ7И	Газизов Александр Тальгатович		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ	Савельев Алексей Олегович	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ст. преподаватель	Потехина Нина Васильевна	-		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ООД	Горбенко Михаил Владимирович	к.т.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ	Губин Евгений Иванович	к.ф-м.н.		

Томск – 2019

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ООП

Код результатов	Результат обучения (выпускник должен быть готов)
Общепрофессиональные компетенции	
Р1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
Р2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.
Р3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.
Профессиональные компетенции	
Р5	Выполнять инновационные инженерные проекты по разработке аппаратных и программных средств автоматизированных систем различного назначения с использованием современных методов проектирования, систем автоматизированного проектирования, передового опыта разработки конкурентно способных изделий.
Р6	Планировать и проводить теоретические и экспериментальные исследования в области проектирования аппаратных и программных средств автоматизированных систем с использованием новейших достижений науки и техники, передового отечественного и зарубежного опыта. Критически оценивать полученные данные и делать выводы.
Р7	Осуществлять авторское сопровождение процессов проектирования, внедрения и эксплуатации аппаратных и программных средств автоматизированных систем различного назначения.
Общекультурные компетенции	
Р8	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.
Р9	Осуществлять коммуникации в профессиональной среде и в обществе в целом, активно владеть иностранным языком, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности, в том числе на иностранном языке.
Р10	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.
Р11	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.04 Программная инженерия (Технологии больших данных)
Отделение информационных технологий

УТВЕРЖДАЮ:
Руководитель ООП
_____ _____ Губин Е.И.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

магистерской диссертсации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	ФИО
8ПМ7И	Газизов Александр Тальгатович

Тема работы:

Разработка программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях	
Утверждена приказом директора (дата, номер)	25.02.2019, 1436/с

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).*	Объектом проектирования является программный комплекс для неявной мультимодальной поведенческой аутентификации в веб-приложениях. Режим работы – непрерывный. Программный комплекс должен предоставлять дополнительный слой аутентификации сторонним веб-приложениям путем анализа нескольких поведенческих характеристик пользователя, причем незаметно для пользователя.
Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	1. Аналитический обзор по теме поведенческой аутентификации 2. Постановка задачи проектирования 3. Разработка программного комплекса 4. Публикация программного комплекса 5. Тестирование программного комплекса 6. Заключение по работе
Перечень графического материала *(с точным указанием обязательных чертежей)*	1. Диаграммы классов модулей программного комплекса

Консультанты по разделам выпускной квалификационной работы *(с указанием разделов)*	
Раздел	**Консультант**
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Потехина Нина Васильевна, ассистент ОСГН
Социальная ответственность	Горбенко Михаил Владимирович, к.т.н., доцент ООД
Обязательное приложение на английском языке	Диденко Анастасия Владимировна, к.ф.н., доцент ОИЯ
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
1 Проектирование биометрической системы	
2 Программная реализация	
3 Публикация системы	
4 Отладка и тестирование системы	
5 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	
6 Социальная ответственность	
7 Biometric system design	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент	Савельев А.О.	к.т.н.		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ПМ7И	Газизов А.Т.		

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.04 Программная инженерия (Технологии больших данных)
Отделение информационных технологий
Период выполнения весенний семестр 2018/2019 учебного года

Форма представления работы:

магистерская диссертация

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
25.02.2019	Проектирование биометрической системы	15
14.03.2019	Программная реализация	20
05.04.2019	Публикация системы	10
14.04.2019	Отладка и тестирование системы	20
15.05.2019	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	10
15.05.2019	Социальная ответственность	10
15.05.2019	Biometric system design	10

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ	Савельев А.О.	к.т.н.		

СОГЛАСОВАНО:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ	Губин Е.И.	к.ф-м.н.		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ПМ7И	Газизову Александру Тальгатовчиу

Школа	ИШИТР	**Отделение школы (НОЦ)**	Отделение информационных технологий
Уровень образования	Магистр	**Направление/специальность**	Программная инженерия (Технологии больших данных)

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих	*Оклад руководителя - 33664 руб.* *Оклад инженера- 21760 руб.*
2. Нормы и нормативы расходования ресурсов	*Дополнительная заработная плата 15%;* *Накладные расходы 16%;* *Районный коэффициент 30%* *Норма амортизации 33%*
3. Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования	*Ставка налоговых отчислений во внебюджетные фонды (30%),*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Оценка коммерческого и инновационного потенциала НТИ	*Анализ конкурентных технических решений* *SWOT-анализ* *Оценка готовности проекта к коммерциализации*
2. Разработка устава научно-технического проекта	*Определение целей и результатов проекта, описание участников проекта*
3. Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок	*Планирование этапов разработки программы, определение трудоемкости их выполнения, построение диаграммы Ганта.* *Расчет сметы затрат на выполнение проекта. Определение рисков и мероприятия по их устранению.*
4. Определение ресурсной, финансовой, экономической эффективности	*Описание потенциального эффекта*
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. Оценочная карта сравнения конкурентных веб-сервисов *2. Матрица SWOT-анализа* *3. Оценка степени готовности научного проекта к коммерциализации* *4. Smart-анализ целей проекта* *5. Календарный план-график проведения работ* *6. Смета затрат* *7. Реестр рисков*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ст. преподаватель ОСГН ШБИП	Потехина Нина Васильевна	-		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ПМ7И	Газизов Александр Тальгатович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬ НАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ПМ7И	Газизову А.Т.

Школа	ИШИТР	**Отделение школы (НОЦ)**	Отделение информационных технологий
Уровень образования	Магистр	**Направление/специальность**	Программная инженерия (Технологии больших данных)

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования и области его применения	Рабочим местом является аудитория №115 10 корпуса Томского политехнического университета. В аудитории рабочей зоной является место за персональным компьютером, отведённое студенту для выполнения работы. Целью работы является разработка программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях. Основным оборудованием, на котором производится работа, является персональный компьютер с периферийными устройствами.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Правовые и организационные вопросы обеспечения безопасности: - специальные правовые нормы трудового законодательства; - организационные мероприятия при компоновке рабочей зоны.	Рабочее место при выполнении работ в положении сидя должно соответствовать требованиям ГОСТ 12.2.032-78. Требования к организации оборудования рабочих мест с ПК регулируется в СанПиН 2.2.2/2.4.1340 – 03.

2. Производственная безопасность 2.1. Анализ выявленных вредных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности: – физико-химическая природа вредности, её связь с разрабатываемой темой; – действие фактора на организм человека; – приведение допустимых норм с необходимой размерностью; – предлагаемые средства защиты. 2.2. Анализ выявленных опасных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности: – механические опасности; – термические опасности; – электробезопасность; – пожаровзрывобезопасность.	Анализ выявленных вредных факторов: • недостаточная освещённость рабочей зоны: отсутствие или недостаток естественного света; • повышенный уровень шума; • повышенный уровень электромагнитных излучений; • повышенная или пониженная влажность воздуха Анализ выявленных опасных факторов: • электрический ток (источником является ПК)
3. Экологическая безопасность: – защита селитебной зоны – анализ воздействия объекта на атмосферу; – анализ воздействия объекта на гидросферу; – анализ воздействия объекта на литосферу; – разработать решения по обеспечению экологической безопасности со ссылками на НТД по охране окружающей среды.	В работе проведён анализ воздействия на атмосферу и гидросферу
4. Безопасность в чрезвычайных ситуациях: – перечень возможных ЧС при разработке и эксплуатации проектируемого решения; – выбор наиболее типичной ЧС; – разработка превентивных мер по предупреждению ЧС; – разработка действий в результате возникшей ЧС и мер по ликвидации её последствий.	В аудиторном помещении возможно ЧС техногенного характера – пожар (возгорание).

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Горбенко Михаил Владимирович	к.т.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ПМ7И	Газизов Александр Тальгатович		

Реферат

Выпускная квалификационная работа содержит 105 страниц машинописного текста, 25 таблиц, 18 рисунков, 1 список использованных источников из 66 наименований, 7 приложений.

Ключевые слова: поведенческая аутентификация, мультимодальная аутентификация, безопасность веб-приложений, разработка программного комплекса.

Объектом исследования является мультимодальная поведенческая аутентификация в веб-приложениях, основанная на фиксированных пользовательских сценариях.

Цель работы – проектирование и разработка программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях.

В процессе исследования спроектирована биометрическая система и разработана архитектура оригинального программного комплекса, предоставляющего веб-приложениям сервис поведенческой аутентификации по статичным пользовательским сценариям. Разработана и опубликована в Интернете исследовательская версия системы, с помощью которой проведен двухнедельный эксперимент с участием 10 человек. По данным первичного эксперимента проведена корректировка системы и рассчитаны параметры ее качества (FRR=6.15%, FAR=0%).

В результате исследования разработан программный комплекс, использующий предложенный метод мультимодальной поведенческой аутентификации по статическим сценариями, который может быть использован в веб-приложениях в качестве дополнительной подсистемы аутентификации.

Область применения: многофакторные системы аутентификации веб-приложений.

Обозначения и сокращения

Термин	Определение
UI	User Interface (пользовательский интерфейс)
FAR	False Acceptance Rate (коэффициент ложного принятия)
FRR	False Rejection Rate (коэффициент ложного отказа)
EER	Equal Error Rate (коэффициент равной ошибки)

Содержание

С.

Введение 14

1. Проектирование биометрической системы 17

1.1. Мультимодальные биометрические системы 18

1.2. Динамики нажатия клавиш 20

1.3. Динамики мыши 23

1.4. Слияние модальностей 25

2. Программная реализация 27

2.1. Архитектура программного комплекса 27

2.2. Модуль ImplicitBio Recorder 28

2.3. Модуль ImplicitBio Server 31

2.3.1. Модели базы данных 32

2.3.2. Классы подмодуля ApplicationServices 33

2.3.3. Контроллеры 35

2.4. Модуль ImplicitBio DemoWeb 36

3. Публикация системы 40

4. Отладка и тестирование системы 43

4.1. Оценка репрезентативности метрик 44

4.2. Выбор пороговой разности успеха метрик 47

4.3. Оценка качества системы 49

5. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение 51

5.1. Предпроектный анализ 52

5.1.1. Анализ конкурентных технических решений 52

5.1.2. SWOT-анализ 53

5.1.3. Метод коммерциализации и оценка коммерческой готовности проекта 55

5.2. Инициация проекта 56
Таблица 12 представляет рабочую группу проекта. 58
5.3. Планирование проектных работ 58
5.3.1. План проекта 58
5.3.2. Бюджет научно-технического исследования 63
5.3.3. Риски проекта 65
5.4. Описание потенциального эффекта 68
6. Социальная ответственность 70
6.1. Правовые и организационные вопросы обеспечения безопасности 70
6.2. Производственная безопасность 72
6.2.1. Недостаточная освещённость рабочей зоны; отсутствие или недостаток естественного света 73
6.2.2. Повышенный уровень шума 76
6.2.3. Повышенный уровень электромагнитных излучений; повышенная напряжённость электрического поля 77
6.2.4. Микроклимат 78
6.2.5. Электрический ток (источник: ПК) 79
6.3. Экологическая безопасность 80
6.4. Безопасность в чрезвычайных ситуациях 81
6.4.1. Пожарная безопасность 81
Заключение 84
Список публикаций студента 85
Список использованных источников 86
Приложение А 90
Приложение Б 91
Приложение В 92
Приложение Г 93

Приложение Е 94

Приложение Ж 95

Приложение З 96

Приложение Е 97

1. Biometric System design 98

1.1. Keystroke dynamics 98

1.2. Mouse dynamics 100

1.3. Multimodal biometric systems 102

1.4. Modalities fusion 104

1.5. Existing web services for behavioural authentication 106

Введение

В современном мире, сосредоточенном вокруг Интернета, вопросы улучшения качества аутентификации и верификации пользователей становятся все более актуальными. Наиболее насущными эти вопросы становятся для веб-приложений, оперирующих с ценной пользовательской информацией, например, онлайн-банкинг. Однако и в менее критичных веб-приложениях, таких как онлайн-форумы или социальные сети, украденная пользовательская сессия может быть использована для распространения вирусов или спама, тем самым нанося вред репутации пользователя, а также связанным системам [1].

Общепринятым подходом для защиты доступа является использование паролей, которые обладают двумя серьезными недостатками: взлом пароля, и его кража [1]. Как только пароль скомпрометирован, злоумышленник может легко использовать аккаунт жертвы, поэтому существует большая потребность в быстрой и точной верификации подлинности текущего пользователя – процессе повторной аутентификации. Существующие распространенные методы верификации и повторной аутентификации требуют непосредственного участия пользователя: это, например, метод ответов на секретные вопросы, сохраненные пользователем ранее, или, более новый метод - двухфакторная аутентификация через получение пользователем секретного кода по email или SMS. Помимо того, что эти методы требуют вовлечения пользователя, они по-прежнему верифицируют пользователя единовременно, т.е. пользовательская сессия впоследствии все равно остается уязвимой. Для быстрого выявления взлома аккаунта необходима более надежная и частая верификация пользователя. При этом, такая верификация должна быть неявной для пользователя, поскольку постоянное его вовлечение в процесс повторной аутентификации будет слишком навязчивым и неудобным [2].

Для улучшения качества аутентификации в целом, а также для повторной аутентификации научным сообществом предлагается использование методов биометрической аутентификации [1-5]. Такие методы используют физиологические и поведенческие биометрические признаки (биометрики) для верификации пользователя. Физиологические биометрики, такие как отпечатки пальцев или сканирование сетчатки, предоставляют точную одноразовую аутентификацию, но требуют специального оборудования, которое может быть дорогим или недоступным для всех пользовательских рабочих станций, также они вовлекают пользователя в процесс аутентификации [1]. С другой стороны, поведенческие биометрики, такие как динамики клавиатуры и мыши, являются довольно многообещающими, потому что они получаются с устройств, которые имеются практически у всех пользователей персональных компьютеров, и, более того, могут быть получены неявно для пользователя [4-7]. Динамики клавиатуры [8-11] и мыши [12-15] по отдельности широко исследовались ранее и показывали свою эффективность в масштабных экспериментах, включающих тысячи людей [2]. Также известен ряд работ [16-18] по их совместному использованию для непрерывной аутентификации пользователя с включением дополнительных биометрик (т.н. мультимодальная аутентификация). Однако гораздо меньше внимания в литературе уделялось мультимодальной поведенческой аутентификации для статических сценариев. При этом в известных работах [19, 20] применение статической биометрической аутентификации ограничивается формой логина либо специальными заданиями, которые требуют непосредственного участия пользователя.

В данной работе предлагается использовать статическую биометрическую аутентификацию в фиксированных пользовательских сценариях взаимодействия с элементами графического интерфейса веб-приложений. Помимо заполнения формы логина, примерами таких сценариев

могут быть заполнение формы на оплату в интернет-банкинге, взаимодействие с меню, написание комментария и т.д. Применение мультимодальной поведенческой аутентификации в рамках фиксированных пользовательских сценариев позволит учесть специфику пользовательского взаимодействия с определенными элементами, и это может быть более эффективным, чем рассмотрение поведения пользователя в целом, как это делается при непрерывной аутентификации. В данной работе будет описана разработка, публикация и первичное тестирование программного комплекса для исследования возможностей мультимодальной поведенческой статической аутентификации по фиксированным пользовательским сценариям в веб-приложениях.

1. Проектирование биометрической системы

Разрабатываемый в данной работе прогаммный комплекс представляет собой мультимодальную биометрическую систему поведенческой аутентификации в веб-приложениях по фиксированным пользовательским сценариям. К системе предъявляются следующие требования:

- система должна предоставлять программный интерфейс для регистрации и аутентификации фиксированных пользовательских сценариев
- система должна легко интегрироваться в различные сторонние веб-приложения
- фиксированные пользовательские сценарии должны задаваться клиентами системы (веб-приложениями) путем объявления элементов графического интерфейса, составляющих пользовательский сценарий
- система должна оперировать с поведенческими биометриками разной природы и не требовать специализированных устройств ввода биометрической информации

Любая биометрическая система, как правило, состоит из 4 модулей (Рисунок 1) [21]. В случае мультимодальной биометрической системы, добавляется модуль слияния биометрических характеристик, который может располагаться в разных местах системы в зависимости от выбранного типа слияния модальностей.

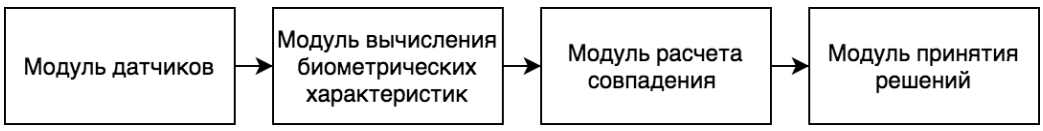


Рисунок 1. Архитектура биометрической системы

Система может работать в двух режимах: регистрация и аутентификация.

1. Во время регистрации пользовательские данные собираются модулем датчика и сохраняются в базу данных.

2. Во время аутентификации происходит вычисление биометрических характеристик и их сравнение с зарегистрированными значениями для получения результата аутентификации. При этом часто применяют адаптацию зарегистрированных биометрических характеристик, которые могут изменяться в течение времени.

В разрабатываемой системе в качестве модуля датчиков выступают тардиционные устройства ввода ПК – клавиатура и мышь. Далее мы рассмотрим актуальность разрабатываемой системы в контексте известных мультимодальных систем, а также выберем для нее биометрические харакетристики и способ их слияния.

1.1. Мультимодальные биометрические системы

Унимодальные биометрические системы доказали свою эффективность в качестве способа дополнительной аутентификации [21]. Однако они имеют ряд свойственных проблем:

1. Шум в воспринятых данных: шум и изменения в биометрической информации могут привести к ложным совпадениям в базе данных.

2. Неуниверсальность: есть некоторые исключения, в которых индивид не может предоставить конкретную биометрию.

3. Внутриклассное изменение: биометрические данные, полученные во время проверки, не будут идентичны данным, используемым для создания шаблона при регистрации для индивидуума.

4. Сходства между классами: это относится к перекрытию пространств признаков, соответствующих нескольким лицам.

5. Ложные атаки: унимодальные системы уязвимы для ложных атак.

Кроме того, на характеристики унимодальной биометрической системы серьезно влияют состояние здоровья пользователей, освещенность, тип датчика и т.д. [21]. Мультимодальная биометрия, которая способна

эффективно преодолеть большинство вышеперечисленных недостатков унимодальных биометрических систем, привлекает внимание многих исследователей [22-24]. Среди преимуществ этих систем:

1. Точность распознавания. Самым непосредственным преимуществом мультимодальной биометрической системы является лучшая точность распознавания.
2. Регистрация биометрических данных. Мультимодальные биометрические системы могут решить проблему неуниверсальности.
3. Конфиденциальность. Мультимодальные биометрические системы повышают устойчивость к определенному типу уязвимостей.

Ахмед и Траоре [22] интегрировали динамики клавиатуры и мыши в единой системе. 22 субъектам было предложено установить систему мониторинга на своих рабочих станциях, которая собирала динамики клавиатуры и мыши. Они запускали программное обеспечение в течение девяти недель. Для каждого пользователя была создана и обучена нейронная сеть. Ahmed et al. показали FAR 0,651% и FRR 1,312%.

Пусара [23] совместил информацию о динамике клавиатуры, мыши и графического интерфейса пользователя в интегрированную архитектуру, которая также может выступать в качестве системы обнаружения взлома. Пусара пригласил 61 добровольца из студентов и аспирантов использовать компьютер под управлением Windows и вести себя нормально, просматривая задание по чтению, а затем отвечая на двадцать вопросов. Окончательные результаты составили FAR 23,37% и FRR 1,50%.

Бейли и соавт. [24] представили поведенческую биометрическую систему, которая объединяет пользовательские данные от взаимодействий клавиатуры, мыши и графического интерфейса пользователя (GUI). Они протестировали систему более чем для 31 пользователя и показали, что слияние модальностей значительно повышают точность аутентификации по

сравнению с отдельными модальностями. Они достигли FAR 2,10% и FRR 2,24%.

Как мы видим, большинство работ, связанных с поведенческой мультимодальной биометрией, посвящены непрерывной аутентификации. Несмотря на универсальность таких систем, они требуют определенного количества времени или действий для принятия решения. Кроме того, они не учитывают, что характеристики динамик клавиатуры и мыши могут зависеть от конкретной задачи, выполняемой пользователем: например, перемещает ли пользователь мышь к кнопке или к полю ввода текста; кликает ли пользователь на кнопку «отменить» или «отправить» и т. д. Статическая аутентификация по фиксированными пользовательским сценариям может учитывать такие факторы и может применяться немедленно после завершения сценария. Однако известные работы для статической аутентификации применимы только для одного сценария (например, форма входа в систему), либо требуют явного графического интерфейса, отвлекающего внимание пользователя. В данной работе предлагается разработка системы для мультимодальной статической поведенческой аутентификации по фиксированным пользовательским сценариям, привязанным к элементам существующего графического интерфейса приложения.

1.2. Динамики нажатия клавиш

Гейнс и соавт. [25] впервые предложили идею использования поведенческой биометрии в качестве дополнения к традиционной аутентификации. Первоначально временны́е данные нажатия клавиш использовались для дополнения ввода пароля [25-29]. В дальнейшем это привело к способности проводить аутентификацию по произвольному тексту [9, 11]. Несмотря на то, что произвольный текст лучше имитирует реальное использование систем, интерес к усилению фиксированных текстов (например, паролей) сохраняется до сих пор [30, 31].

Как правило, необработанные данные о нажатии клавиш собираются посредством регистрации пользовательских событий «keydown» и «keyup». Выполняя простые математические операции с метками времени, полученными из необработанных данных нажатия клавиш, можно получить длительность или интервал между последовательными нажатиями клавиш. Информация о времени двух последовательных нажатий клавиш, более известная как дираф, является основной характеристикой данных, представленных в области динамики нажатий клавиш [11]. Он широко подразделяется на два типа, а именно: время задержки (*Dwell Time*) и время полета (*Flight Time*) - Рисунок 2.

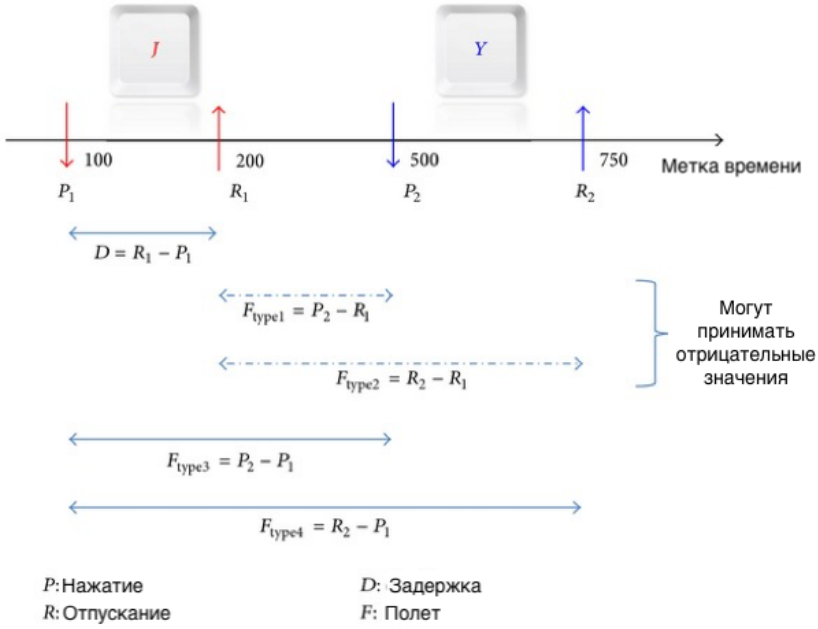


Рисунок 2. Различные события нажатия клавиш двух символов «J» и «Y» наряду с формированием времени задержки (D) и времени полета (F).

Время задержки (DT) определяется как промежуток времени между нажатием и отпусканием одной клавиши. Другими словами, как долго была нажата клавиша. DT можно рассчитать по формуле

$$DT_n = R_n - P_n,$$

где *R* и *P* обозначают метку времени отжатия и нажатия клавиши соответственно, а *n* обозначает позицию предполагаемого DT. Количество DT всегда будет равно длине введенной строки.

Время полета (FT) определяется как промежуток времени между отжатием и нажатием двух последовательных клавиш. FT может существовать в четырех различных формах, как это показывает Рисунок 2. Формулы для расчета каждой формы представлены ниже:

$$FT_{type1,n}=P_{n+1}-R_n,$$
$$FT_{type2,n}=R_{n+1}-R_n,$$
$$FT_{type3,n}=P_{n+1}-P_n,$$
$$FT_{type4,n}=R_{n+1}-P_n,$$

где *R* и *P* указывают отметку времени отжатия и нажатия символа соответственно, а *n* указывает положение предполагаемой FT. В отличие от DT, количество сгенерированных FT всегда будет на единицу меньше длины заданной строки. Каждый тип времени полета дает аналогичную информацию о нажатии клавиш, и неизвестно, какая метрика лучше [32].

N-граф является метрикой измерения времени между тремя или более последовательными событиями нажатия клавиш. Он определяется как время, прошедшее между нажатием клавиши и *n*-ным событием нажатия клавиши.

В [32] авторы отмечают, что в 80% научных работ использовались диграфы; 7% использовали триграф; только 4% использовали n-граф. Наиболее вероятной причиной популярности диграфа является возможность генерировать значительно больше экземпляров временных векторов. Таким образом, любое значение *n*, большее 3 (триграф), выбиралось редко, за исключением экспериментов, в котором использовалось огромное количество входного текста. В данной работе мы будем использовать диграф и наиболее распространенные характеристики нажатия клавиш, такие как время полета и задержки для анализа фиксированных текстов.

1.3. Динамики мыши

Динамики мыши активно исследуются для поведенческой аутентификации [20, 33]. С тех пор как Эверит и МакОван [34] впервые исследовали, могут ли пользователи различаться по стилю их работы с мышью, было предложено несколько подходов к статической аутентификации на основе динамик мыши [35].

Хашиа и соавт. [36] представили схему входа в систему, основанную на движениях мыши, с использованием двухэтапного подхода, при котором фазы регистрации и тестирования включают перемещение указателя мыши между парами точек, последовательно отображаемых на экране. Данные собирались от 15 участников в контролируемой среде, и EER составил 15%, а время аутентификации - 20 секунд.

Боурс и соавт. [37] описали метод входа в систему для доступа к компьютерным системам на основе движений мыши в неконтролируемой среде с 28 участниками. Участникам их исследования было предложено сыграть в лабиринт с заранее заданным путем. Эксперимент с 28 участниками дал EER=26,8%, время аутентификации неизвестно.

Гамбоа и соавт. [38] представили статическую систему аутентификации для веб-приложения, основанную на движениях мыши, когда пользователь вводит PIN-код. В предложенной схеме система отображала виртуальную клавиатуру на экране и требовала, чтобы пользователи использовали только мышь для ввода пары имя пользователя-пароль. Эксперименты с 50 участниками дали EER=6,2% на основе 15 движений мыши.

Недавно Revett и соавт. [39] представили систему статической аутентификации на основе динамики мыши, названную «Mouse-Lock», в которой пользователь проходил аутентификацию с помощью графического комбинированного графического интерфейса в виде замка с иконками,

расположенными на круговом циферблате. Эксперимент с 6 участниками дал средний FAR=3,5% и FRR=4%.

Таблица 1 представляет характеристики динамик мыши, использованные в известных работах по статической поведенческой аутентификации.

Таблица 1. Поведенческие харакетристики динамик мыши

Характеристика	**Описание**
Расстояние	Расстояние между двумя последовательными позициями мыши при клике.
Смещение движения	Расстояние между реальной траекторией мыши и идеальной
Время двмжения мыши	Интервал времени между начальной и конечной точкой движений мыши.
x-скорость	Скорость движения в направлении абсциссы.
y-скорость	Скорость движения в направлении ординат.
x-скорость к расстоянию	Скорость движения по сравнению с пройденным расстоянием в направлении абсциссы.
y-скорость к расстоянию	Скорость движения по сравнению с пройденным расстоянием в направлении ординат.
Средняя скорость к расстоянию	Средняя скорость движения по сравнению с накопленным пройденным расстоянием.
x-ускорение	Ускорение движения в направлении абсциссы.
y-ускорение	Ускорение движения в направлении ординат.
x-ускорение к расстоянию	Ускорение движения по сравнению с пройденным расстоянием в направлении абсциссы
y-ускорение к расстоянию	Ускорение движения по сравнению с пройденным расстоянием в направлении ординат
Ускорение к расстоянию	Среднее ускорение движения по сравнению с накопленным пройденным расстоянием.
Задержка перед кликом	Средняя длина временного интервала между последним событием движения мыши и событием клика
Линейный угол	Угол между горищонталью и линейным приближением направления движения мыши

В данной работе для анализа динамик мыши будут использоваться следующие характеристики: задержка перед кликом (*delayBeforeClick)*, линейный угол (*linearAngle*), средняя скорость (*avgSpeed*), среднее ускорение (*avgAcceleration*).

1.4. Слияние модальностей

Слияние в биометрических системах может происходить путем слияния признаков, слияния реузльтатов совпадений или слияния решений от каждой отдельной модальности [40, 41].

При слиянии на уровне признаков (Рисунок 3) сигналы сначала обрабатываются, а векторы признаков извлекаются отдельно от каждой биометрической характеристики. После этого эти векторы признаков объединяются для формирования составного вектора признаков, который затем используется для классификации [41].

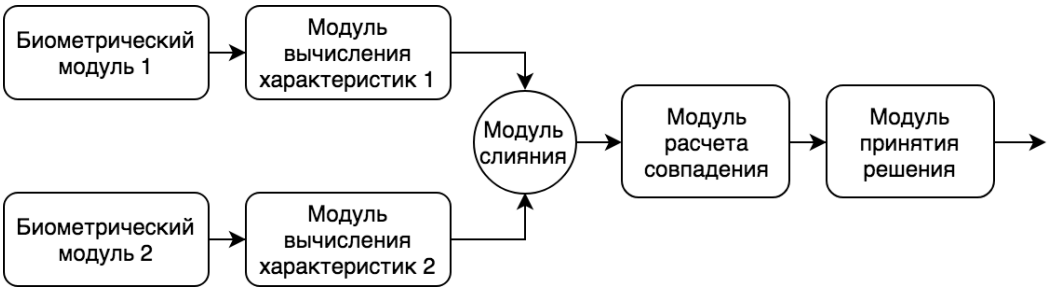


Рисунок 3. Слияние на уровне признаков.

При слиянии на уровне результатов совпадений, вместо объединения векторов признаков, они обрабатываются отдельно, и для каждого отдельно определяется результат совпадения, и затем эти результаты объединяются для классификации (Рисунок 4). Для объединения результатов совпадений могут быть использованы различные статистические методы обучения [41].

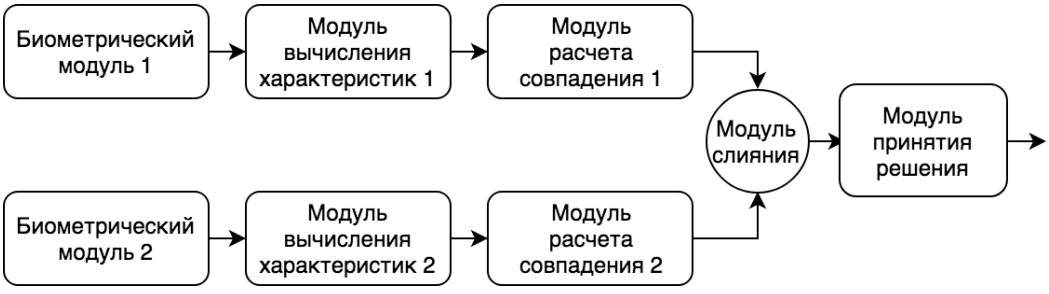


Рисунок 4. Слияние на уровне результатов совпадений.

При слиянии на уровне принятия решений каждая модальность классифицируется независимо, а окончательная классификация основана на

объединении результатов различных модальностей (Рисунок 5). Другими словами, для принятия окончательного решения учитывается конечное решение каждой биометрической модальности [41].

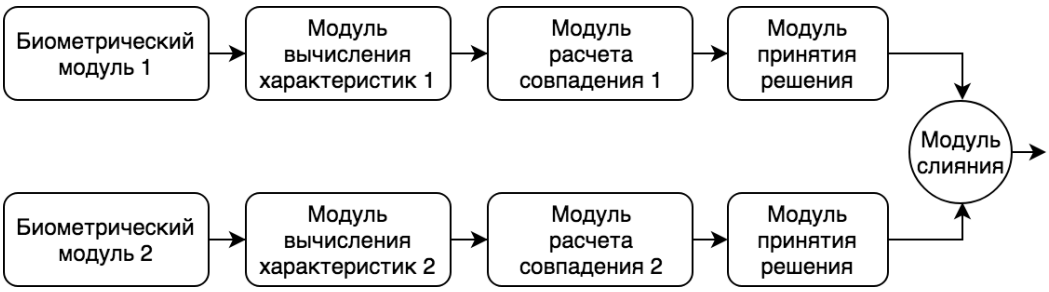


Рисунок 5. Слияние на уровне решений.

В данной работе для слияния поведенческих модальностей используется слияние на уровне решений, поскольку оно является наиболее простым в реализации и может также применяться на уровне отдельных элементов сценария.

2. Программная реализация

2.1. Архитектура программного комплекса

Разрабатываемый программный комплекс (далее – *ImplicitBio*) в форме конечного продукта является веб-сервисом для дополнительной аутентификации пользователей различных веб-приложений (далее – клиент-приложения) по их биометрическим поведенческим характеристикам при определенных сценариях взаимодействия пользователей с клиент-приложением.

Диаграмма работы системы (Рисунок 6) описывает взаимодействие компонентов системы *ImplicitBio* с клиентской и серверной частью конкретного клиент-приложения.

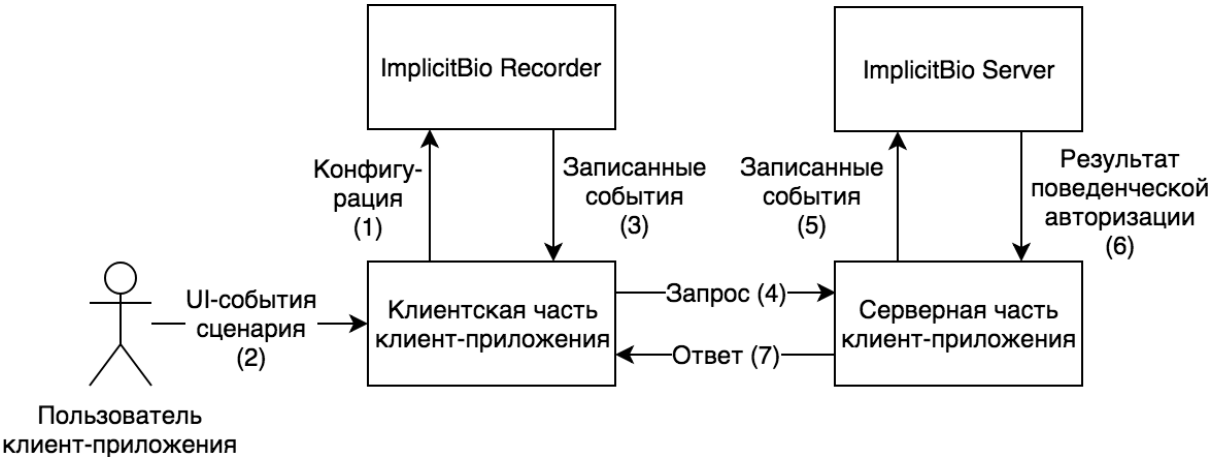


Рисунок 6. Диаграмма работы системы *ImplicitBio*

Клиентская часть клиент-приложения загружает и инициализирует модуль *ImplicitBio Recorder* с конфигурацией (1), соответствующей определенному пользовательскому сценарию (например, заполнение формы аутентификации) и происходит запись (2) событий (далее – UI-события) пользовательского интерфейса. При отправке клиент-приложением данных сценария (например, при отправке формы) на свой сервер (4), он также отправляет и записанные с помощью *ImplicitBio Recorder* UI-события (3) этого сценария. Серверная часть клиент-приложения отсылает полученные UI-события на *ImplicitBio Server*, где происходит построение поведенческого

биометрического профиля, который сравнивается с зарегистрированным ранее, и серверу клиент-приложения возвращается ответ с результатом поведенческой аутентификации. Таким образом, система *ImplicitBio* обеспечивает легкую интеграцию с произвольным веб-приложением и прозрачность собираемых пользовательских данных.

В рамках данной работы разрабатывается упрощенная исследовательская версия системы *ImplicitBio* предоставляющая две функции: «Публичное демо» и «Закрытое тестирование». «Публичное демо» заключается в быстрой публичной демонстрации вычисления близости двух попыток прохождения определенного сценария с развернутым отчетом по компонентам. «Закрытое тестирование» заключается в возможности многократного прохождения сценария определенным пользователем с сохранением данных в базе для их дальнейшего анализа и принятия решений по корректировке компонент аутентификации и алгоритмов их слияния. Отличие от описанной продуктовой версии системы *ImlicitBio* (Рисунок 6) в том, что клиент-приложением будет являться конкретный собственный модуль *ImplicitBio DemoWeb*, для простоты взаимодействующий напрямую с *ImplicitBio Server* (отсутствует серверная часть клиент-приложения), который в свою очередь будет содержать методы, специфичные для демонстрации и тестирования.

2.2. Модуль ImplicitBio Recorder

Модуль *ImplicitBio Recorder* системы *ImplicitBio* предназначен для сбора UI-событий в рамках определенных пользовательских сценариев. Данный модуль представляет собой JavaScript-библиотеку, подключаемую на HTML-страницу клиент-приложения. Библиотека разработана с использованием возможностей стандарта ECMAScript 2015, позволяющего использовать синтаксис классов. Диаграмма классов библиотеки представлена в Приложении А (здесь и далее в диаграммах используется синтаксис

TypeScript). Клиентской части клиент-приложения предоставляется класс *ImplicitBioStaticRecorder,* объекты которого соответствуют определенному пользовательскому сценарию. Пример создания объекта для сценария заполнения формы аутентификации представлен в Листинге 1.

Листинг 1.

```
this.authFormRecorder = new ImplicitBioStaticRecorder({
  scenarioId: 'simpleForm',
  elements: [
    {
      name: 'login',
      type: 'input',
      cssId: 'login'
    },
    {
      name: 'password',
      type: 'input',
      cssId: 'password'
    },
    {
      name: 'submitButton',
      type: 'button',
      cssId: 'submit-button'
    },
  ],
})
```

В конструктор *ImplicitBioStaticRecorder* передается объект с полями *scenarioId* (идентификатор сценария) и *elements*, содержащим массив объектов-описаний элементов графического интерфейса, участвующих в сценарии: в данном случае (Листинг 1), это поля ввода для логина и пароля, а также кнопка отправки формы. В каждом объекте-описании указывается уникальное имя элемента, его тип (поле ввода или кнопка), а также CSS-идентификатор, позволяющий найти этот элемент на HTML-странице. По указанным объектам-описаниям объект *ImplicitBioStaticRecorder* инициализирует экземпляры *ImplicitBioElementRecorder* и агрегирует их в приватном поле *_elements*. После инициализации объекта производится сохранение UI-событий с указанных элементов, а также событий мыши. Когда пользовательский сценарий завершен (в данном случае при отправке формы), клиент-приложение может получить записанные события вызовом публичного метода *getRecordedEvents* у объекта, инициализированного ранее

и передать их для регистрации или аутентификации по поведенческим признакам модулю *ImplicitBio Server*. Клиент-приложение также может выполнить удаление всех записанных событий с помощью публичного метода *clearRecordedEvents*. Данные записанных событий представляют собой массив объектов, реализующих обобщенный интерфейс *RawUIEvent* (описанный в Приложении А) и хранящих данные о типе события, элемента, на котором это событие произошло, а также специфичные данные о событии (например, координаты мыши или код клавиши).

Следует отметить, что в конкретном сценарии отправки формы, можно избежать непосредственного вызова метода *getRecordedEvents* клиент-приложением: например, библиотека может сама создать скрытое поле на форме и заполнять его собираемыми данными. Таким образом, данные автоматически отправятся на сервер клиент-приложения при отправке формы. Однако такой вариант будет работоспособен только в этом конкретном сценарии и, более того, только в традиционных веб-приложениях, в которых происходит перезагрузка страницы при отправке формы. Выделение отдельного метода *getRecordedEvents* позволяет клиент-приложению конфигурировать произвольные пользовательские сценарии, самостоятельно определяя их завершение. В любом случае, в дальнейшем нетрудно создать отдельные классы для конкретных пользовательских сценариев, расширяющие обобщенный *ImplicitBioStaticRecorder.*

Также следует отметить, что разработанный модуль может быть использован не только для неявной поведенческой аутентификации (т.е. с использованием уже существующих в клиент-приложении элементов пользовательского интерфейса), но и для явной – в случае создания отдельных UI-сценариев, поставляемых вместе с библиотекой, которые позволяют записывать более уникальные профили пользователей, и, следовательно, дают лучшую точность. Примером сценария для явной поведенческой

аутентификации может быть последовательное нажатие нескольких кнопок [5].

2.3. Модуль ImplicitBio Server

Модуль *ImplicitBio Server* системы *ImplicitBio* является основной ее частью и предназначен для обработки запросов регистрации и аутентификации определенного сценария по поведенческому профилю, формируемому по UI-событиям, собранным с помощью модуля *ImplicitBio Recorder*. Исходный код модуля написан на языке TypeScript, который предоставляет статическую типизацию и компилируется в JavaScript. Рассмотрим диаграмму работы модуля *ImplicitBio Server* (Рисунок 7): программный модуль представляет собой NodeJS приложение, предоставляющее интерфейс по HTTP протоколу с помощью библиотеки ExpressJS. Контроллеры ExpressJS являются входной точкой для модуля. В качестве базы данных используется нереляционная база MongoDB: она была выбрана в связи с необходимостью хранить большое количество разнородных данных (пользовательских событий), а также в связи с наличием для нее удобной ORM-библиотеки Mongoose. Классы для создания и сравнения поведенческих профилей пользовательских сценариев вынесены в подмодуль *ApplicationServices*, чтобы избежать высокой связности с классами моделей для базы данных.

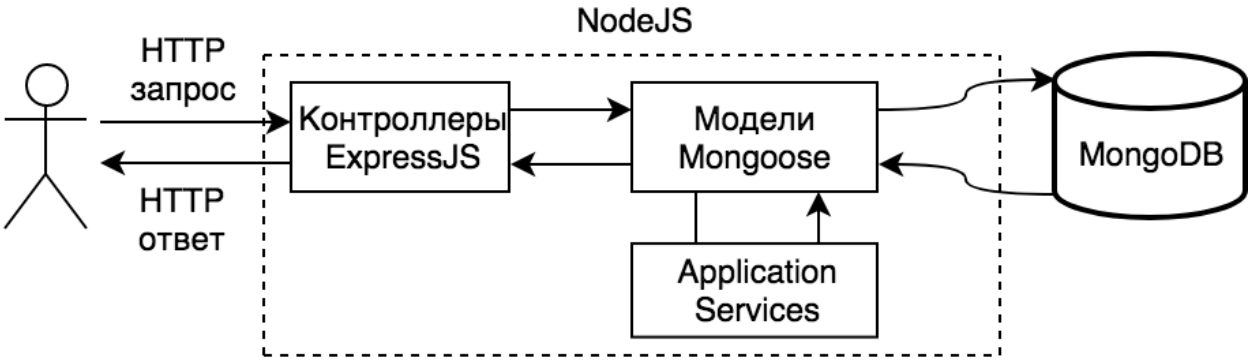


Рисунок 7. Диаграмма работы модуля *ImplicitBio Server.*

2.3.1. Модели базы данных

Модели, используемые при операциях с базой данных, определяются через классы TypeScript с использованием библиотеки Mongoose. Использование ORM-библиотеки позволяет определить свойства и методы для создаваемых объектов, а также специальные методы, выполняемые на различных этапах работы базы данных, например, перед сохранением объекта. Диаграмма моделей сущностей, хранимых в базе данных представлена в **Приложении Б**. Каждая из моделей *ClientApp*, *ClientAppUser* и *UIInteraction* соответствует коллекции (корневому узлу) в MongoDB и ссылается на предыдущую по идентификатору, образуя последовательные отношения 1 ко многим. Модель *UIInteraction* соответствует прохождению пользователем определенного сценария (взаимодействию со страницей) и агрегирует произошедшие при этом UI-события в поле *uiEvents,* используя возможность хранения встраиваемых под-документов в MongoDB. Таким образом, фактически в базе данных хранятся исходные пользовательские события, отправленные модулем *ImplicitBio Recorder*. Эти данные являются входными для вычисления поведенческого профиля пользователя, который впоследствии используется для аутентификации. Хранение исходных данных о низкоуровневых UI-событиях вместо параметров поведенческих профилей обусловлено исследовательской спецификой работы: параметры профиля, а также алгоритм их слияния подлежат уточнению после разработки системы. При хранении исходных данных, возможно сравнение эффективности системы при использовании различных биометрических признаков, а также способов их слияния.

Экземпляры *UIInteraction* создаются через статический метод-фабрику *UIInteraction.createFromRawEvents*. Статический метод *UIInteraction.getSimilarityReport* с помощью классов из подмодуля *ApplicationServices* позволяет получить отчет о степени близости двух

экземпляров *UIInteraction* и конечный результат поведенческой аутентификации.

2.3.2. Классы подмодуля ApplicationServices

Диаграмма классов подмодуля *ApplicationServices* представлена в Приложении В. Таблица 2 представлает их краткое описание.

Таблица 2. Краткое описание классов подмодуля *ApplicationServices*

Имя класса	Краткое описание
UIInteractionFeature	Поведенческий профиль, соответствующий конкретному пройденному пользовательскому сценарию
BioFeatureBase	Базовый класс, наследуемый всеми классами биометрических характеристик
ButtonBioFeature	Биометрические характеристики взаимодействия с кнопкой
InputBioFeature	Биометрические характеристики взаимодействия с полем ввода
MouseMovementFeature	Биометрические характеристики движения мыши

Подмодуль предоставляет класс *UIInteractionFeature*, инкапсулирующий создание объекта мультимодального поведенческого профиля по исходному экземпляру *UIInteraction* и его последующее сравнение с объектом того же класса через публичный метод *compare*. Основной ролью класса *UIInteractionFeature* является создание и агрегация в поле *elementsFeatures* экземпляров классов *ButtonBioFeature* и *InputBioFeature*, хранящих метрики взаимодействия с определенным элементом пользовательского интерфейса. Метод *compare* по существу возвращает объект с результатом вызовов методов *compare* для каждого элемента из *elementsFeatures*.

Взаимодействие пользователя с графическим интерфейсом разделяется на взаимодействие с кнопками (класс *ButtonBioFeature*) и полями ввода с клавиатуры (класс *InputBioFeature*). В начальной версии системы, в качестве метрик для кнопки выбраны признак движения мыши к кнопке (поле *enterToElement*, хранящее экземпляр класс *MouseMovementFeature*) и временная задержка перед кликом (поле *delayBeforeClick*). В качестве метрик

для поля ввода выбраны также признак движения мыши к полю (*enterToElement*), временная задержка перед фокусом поля (*delayBeforeFocus*), а также временные признаки нажатия клавиш: массив длительностей зажатия каждой клавиши (*dwellTimes*) и массив временных интервалов между нажатием двух последовательных клавиш (*flightTimes*).

Класс *MouseMovementFeature* имеет статичный публичный метод-фабрику *createMousemovementsFromEvents*, для создания массива собственных экземпляров из набора UI-событий. Каждый экземпляр *MouseMovementFeature* соответствует последовательному непрерывному движению мыши, из которого в качестве поведенческих признаков в начальной версии системы вычисляются параметры скорости, расстояния и линейного угла траектории движения мыши. Статичный метод *findMouseMovementBeforeEvent* используется для нахождения ближайшего по времени движения мыши перед определенным событием (например, фокусом поля) и последующего вычисления временной задержки перед этим событием.

Каждый из классов *ButtonBioFeature*, *InputBioFeature*, *MouseMovementFeature* наследуется от абстрактного класса *BioFeatureBase*, содержащего общие для дочерних поля и методы. Поле *events* хранит исходные события, из которых вычислялись поведенческие метрики. В конструкторе производится вызов *validateEvents* и *calculateFeatureValues*. *BioFeatureBase* также содержит статические методы, лежащие в основе вычисления методов *compare* дочерних классов (результата аутентификации): это *compareNumberProperty* для сравнения числовых значений и *compareNumbersArrays* для сравнения числовых массивов. Эти методы используют вычисление относительной разности чисел и сравнивают ее с *maxSuccessDiff*, определяя результат аутентификации *isSuccess*. Метод *compare* возвращает объект интерфейса *IMultiCompareResult*, агрегирующий в себе многокомпонентный результат аутентификации для каждого компонента в отдельности (в поле *components*), а также счетчик слияния авторизаций этих

компонент (в поле *successCount*). Для удобства первоначальной отладки системы, *ICompareResult* содержит поля *a* и *b* – соответствующие значениям двух сравниваемых метрик.

Для получения итогового результата аутентификации используется слияние биометрик на уровне решения, описанное ранее в первой главе. При сравнении двух поведенческих профилей на низшем уровне метрик с помощью коэффициентов пороговой разности успеха *maxSuccessDiff* вычисляется булево значение *isSuccess*. На каждом уровне выше опредялется счетчик *successCount*, который имеет нулевое начальное значение и вычисляется проходом по дочерним узлам: если узел имеет свой *successCount*, то он прибавляется к текущему, в противном случае используется *isSuccess* для увеличения либо уменьшения *successCount.* В последнем случае абсолюное значение приращения может зависить от веса метрики: например, веса метрик *dwellTimes* и *flightTimes* ввиду их относительной сложности выбраны равными 2, а всех остальных – 1. Таким образом, значение *successCount* на верхнем уровне позволяет судить об успешности попытки аутентификации. Принимается, что неотрицательное значение означает, что биометрическая аутентификация прошла успешно. Описанный алгоритм слияния позволяет проводить сравнение биометрических профилей с произвольным количеством и уровнем вложенности элементов и метрик.

2.3.3. Контроллеры

ImplicitBio Server содержит два контроллера, обрабатывающих входные HTTP-запросы: *client-app-user* для управления данными о пользователях клиент-приложения, и *static-auth* для обработки запросов статичной аутентификации. Контроллер *client-app-user* содержит методы для регистрации пользователя, а также для аутентификации и деаутентификации для дифференциации попыток прохождения сценариев по пользователям для

функции «Закрытое тестирование». Контроллер *static-auth* содержит два метода: *publicDemo* и *privateTesting*.

Метод *publicDemo* принимает данные сценария, собираемые *ImplicitBio Recorder* и при первой попытке возвращает поведенческий профиль сценария, а при второй – мультимодальный отчет о близости двух попыток. При этом, после второй попытки все связанные данные удаляются.

Метод *privateTesting* позволяет отправить данные сценария зарегистрированному и авторизованному ранее пользователю и сохраняет их в базе, проверяя при этом поля на идентичность значений, записанных ранее.

2.4. Модуль ImplicitBio DemoWeb

Модуль *ImplicitBio DemoWeb* представляет собой клиентскую часть разрабатываемого веб-приложения для исследования мультимодальной поведенческой статичной аутентификации. Этот модуль написан с использованием технологий HTML, CSS и JavaScript и является независимым компонентом, предоставляющим одностраничное клиентское приложение (имеет единственный файл расширения HTML). Рисунок 8 представляет главный экран приложения.

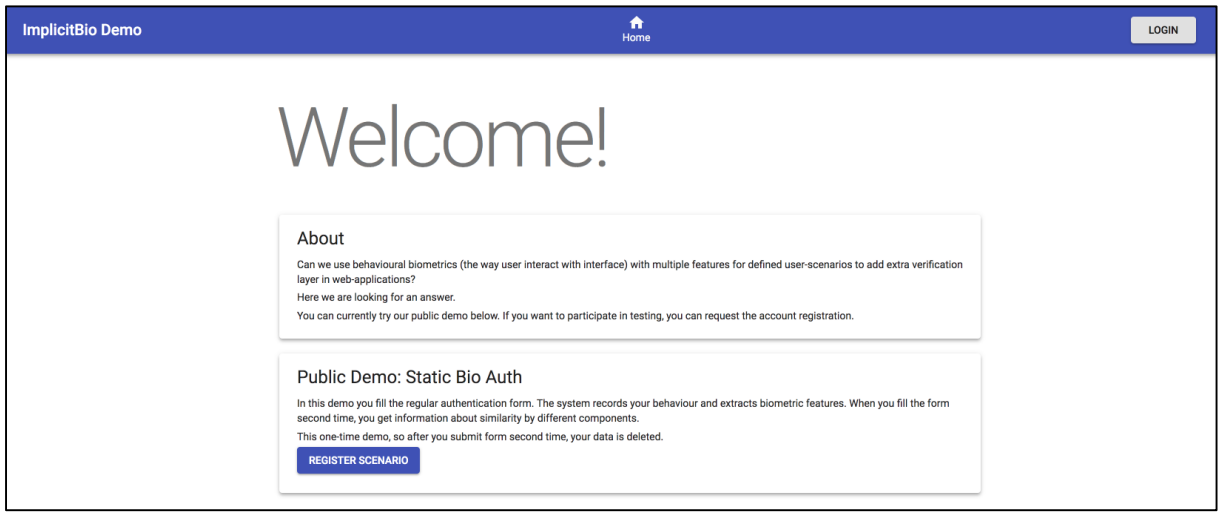


Рисунок 8. Главный экран *ImplicitBio DemoWeb*

На нем, в рамках функции «Публичное демо», пользователю предоставляется возможность пройти сценарий заполнения формы

аутентификации. При клике на кнопку «Register Scenario» открывается экран прохождения сценария (Рисунок 9), с помощью модуля *ImplicitBio Recorder* начинается запись пользовательских событий.

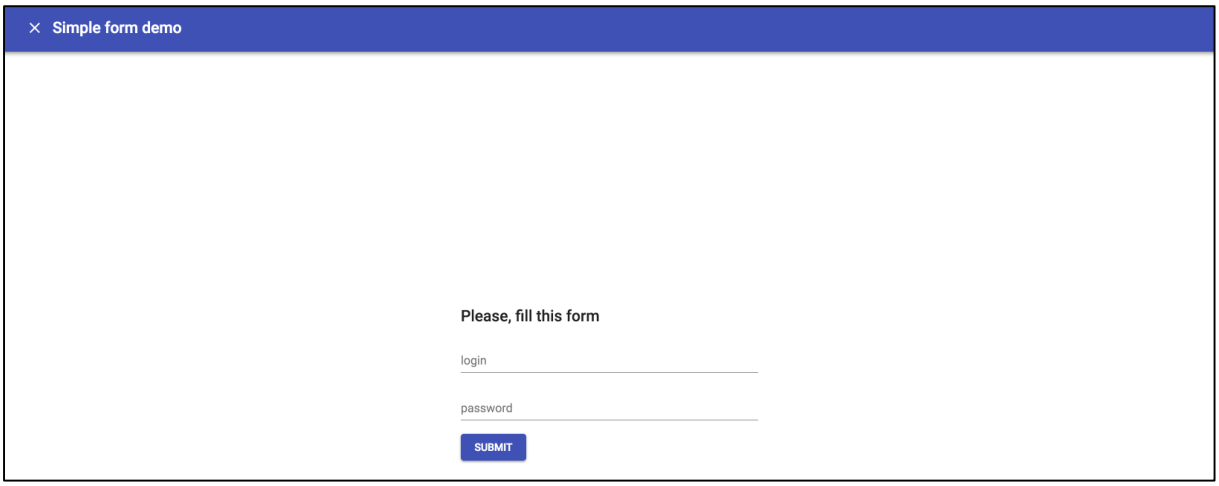


Рисунок 9. Экран прохождения сценария заполнения формы аутентификации

При клике на кнопку «Submit», происходит HTTP запрос к удаленному методу *publicDemo* модуля *ImplicitBio Server*, экран прохождения сценария закрывается, и отображаются данные ответа от сервера: в поле *interactionFeature* выводятся данные зарегистрированного профиля – это объект класса *UIInteractionFeature* (Рисунок 10). При этом кнопка «Register Scenario» меняется на «Authenticate Scenario».

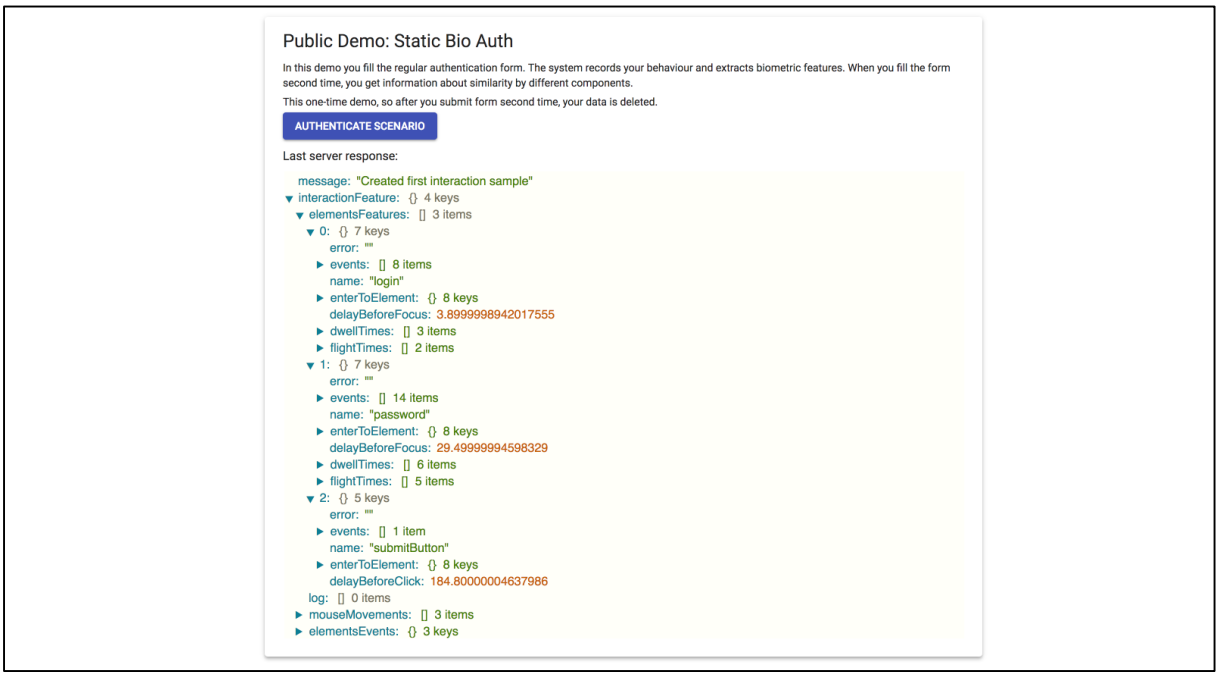


Рисунок 10. Главный экран после 1-го прохождения сценария.

При нажатии на кнопку «Authenticate Scenario», снова открывается тот же экран (Рисунок 9). После его прохождения во 2-ой раз, происходит тот же запрос к серверу, и снова открывается главный экран (Рисунок 11), где теперь в ответе от сервера в поле *similarityReport* приходит отчет сравнения нового профиля с предыдущим - объект интерфейса *IMultiCompareResult*.

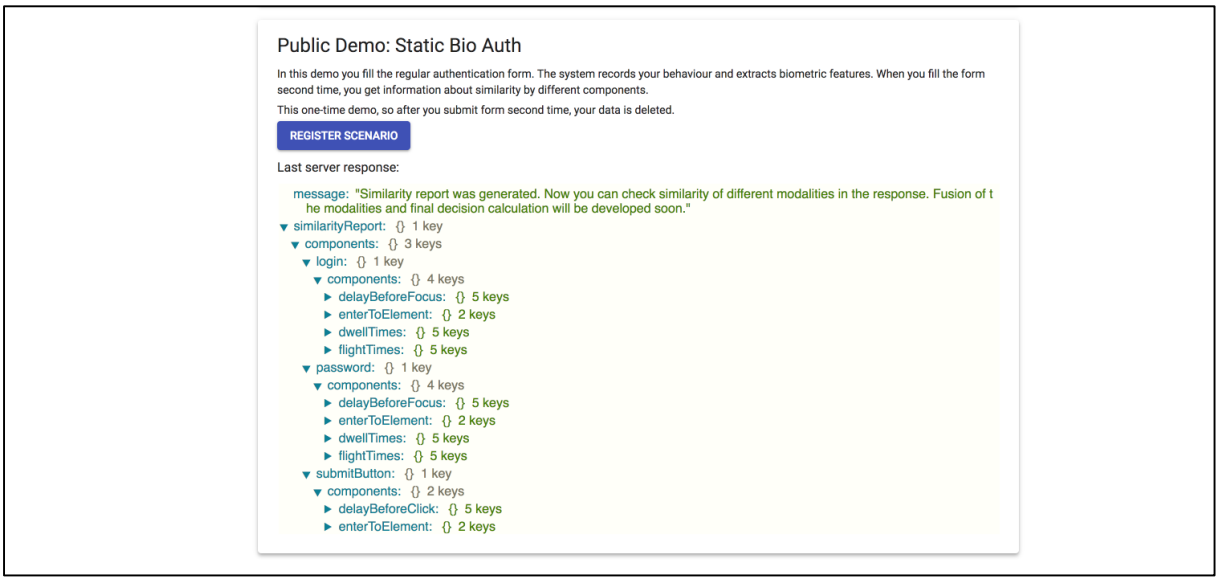


Рисунок 11. Главный экран после 2-го прохождения сценария.

Рисунок 11 представляет объект отчета до 4-ого уровня вложенности свойств, полностью этот же объект представлен в Приложении В. По нему видно, что некоторые метрики дали положительный результат (значение *isSuccess*, равное *true*), а некоторые – отрицательный. В начальной версии системы по умолчанию для каждой метрики используется одинаковый порог разности успеха, равный 0,15, который подлежит уточнению для каждой метрики после проведения экспериментов.

Использование функции «Публичное демо» хорошо подходит для демонстрации возможностей системы, а также быстрой отладки ее модулей при их разработке и изменении. Однако для исследования эффективности различных способов вычисления близости метрик, а также способов их слияния, необходимо провести анализ применения различных параметров для поведенческих сценариев различных пользователей. Для дальнейшего проведения подобного сбора данных разработана функция «Приватное тестирование» веб-приложения *ImplicitBio DemoWeb*. Она позволяет авторизоваться зарегистрированному пользователю и проходить сценарии, данные которых будет сохраняться в базе для дальнейшего анализа. Рисунок 12 представляет экран «Приватное тестирование» для авторизованного пользователя с логином «bbm». Кнопка «Start» работает аналогично кнопке «Register scenario», но после прохождения сценария система делает запрос к методу *privateTesting* контроллера *ImplicitBio Server* и сохраняет данные за текущим пользователем, не выводя при этом ответ от сервера на страницу.

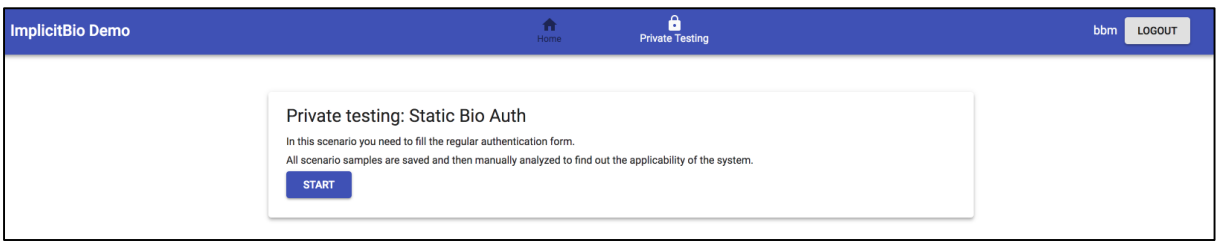


Рисунок 12. Экран «Приватное тестирование»

3. Публикация системы

Для возможности проведения эксперимента необходимо опубликовать разработанные модули *ImplicitBio DemoWeb* и *ImplicitBio Server* в Интернете. Основным моментом в публикации веб-приложения является выбор веб-хостинга. Для уменьшения временных затрат целесообразно выбрать такой веб-хостинг, который предоставляет готовые виртуальные сервера с уже установленными технологиями проекта (в нашем случае это среда исполнения *Node.js* [42]). Для этого выбран популярный сервис *DigitalOcean*, который предоставляет облачные услуги для разработчиков, дает возможность развертывать и масштабировать приложения одновременно на нескольких компьютерах [43]. В *DigitalOcean* арендуется виртуальный сервер (1 ГБ ОЗУ, 25 ГБ ПЗУ) с предустановленным образом “Ubuntu NodeJS 6.12.3 on 16.04”, в котором помимо среды *Node.js* также установлен веб-сервер *nginx* [44]. Монорепозиторий проекта, содержащий все разработанные модули, клонируется с сервера *Bitbucket* [45] на сервер *DigitalOcean*.

Модуль *ImplicitBio Server* представляет собой веб-сервер на *Node.js* взаимодействующий с БД *MongoDB*. Для упрощения процедуры разворачивания и настройки БД, используется база данных как сервис с помощью услуг *mLab* – дочерней компании *MongoDB* [46]. Этот сервис берет на себя обязанности хостинга БД, ее поддержки, масштабирования и мониторинга (Рисунок 13). Mlab предоставляет бесплатный план при объеме данных до 0.5 ГБ, чего достаточно для проведения эксперимента. Таким образом, для работоспособности БД в боевом окружении достаточно лишь сменить данные для доступа к БД.

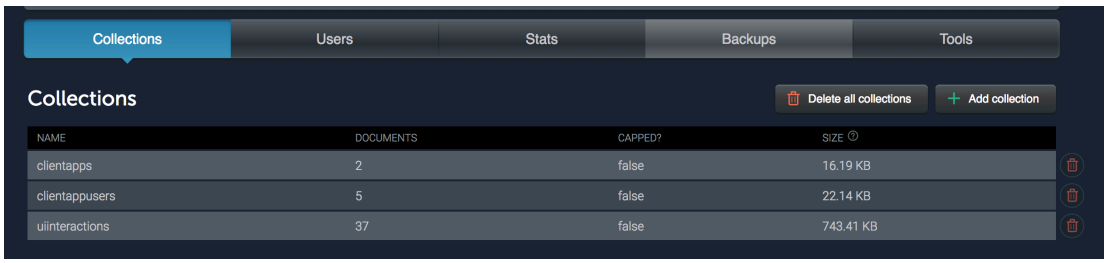


Рисунок 13. Структура БД модуля *ImplicitBio Server* в графическом интферфейсе сервиса *mLab*.

Сам веб-сервер *ImplicitBio Server* можно запустить в качестве процесса используя непосредственно среду исполнения *Node.js*, однако это не позволит конфигурировать его поведение и отслеживать состояние, а также приведет к неработоспособности сервера при возникновении необработанных ошибок процесса без какого-либо легирования и автоматического восстановления. Для решения этих проблем используется *pm2* – менеджер процессов *Node.js* [47]. Запуск веб-сервера через *pm2* позволяет отслеживать его статус и детальную информацию (Рисунок 14). Веб-сервер *ImplicitBio Server* запускается на 3003 порту, на который с помощью *nginx* проксируются запросы по адресу */projects/implicitbio-server*. Модуль *ImplicitBio DemoWeb* представляет собой статический веб-сайт, который доставляется непосредственно веб-сервером *nginx*. Рисунок 15 содержит фрагмент файла конфигурации *nginx* для публикации модулей *ImplicitBio Server* и *ImplicitBio DemoWeb*. При изменении исходного кода проекта, для обновления системы, необходимо обновить копию репозитория на сервере *DigitalOcean*, и перезапустить процесс модуля *ImplicitBio Server*.

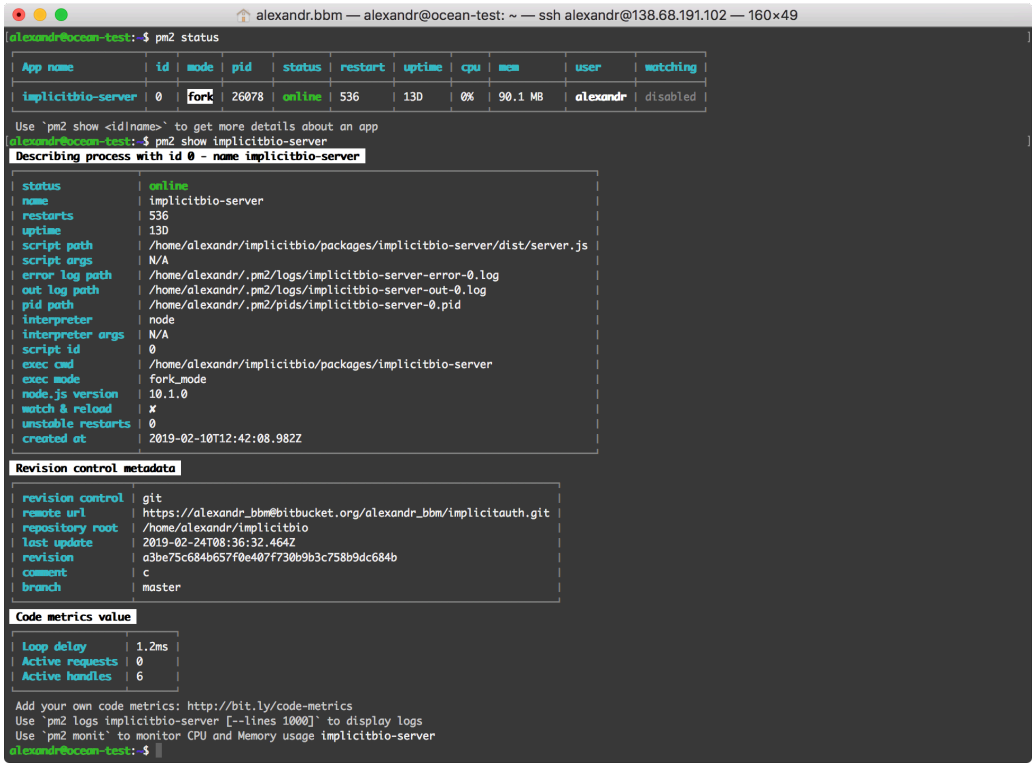


Рисунок 14. Отчет *pm2* о состоянии процесса *ImpicitBio Server*

```
location /projects/implicitbio {
         alias /home/alexandr/implicitbio/packages/implicitbio-demo-web/build;
         index index.html;
 }

location /projects/implicitbio-server {
         proxy_pass http://localhost:3003;
         proxy_http_version 1.1;
         proxy_set_header Upgrade $http_upgrade;
         proxy_set_header Connection 'upgrade';
         proxy_set_header Host $host;
         proxy_cache_bypass $http_upgrade;
 }
```

Рисунок 15. Конфигурация *nginx* для *ImplicitBio Server* и *ImplicitBio DemoWeb*

Таким образом, система опубликована в Интернете и доступна по адресу https://agazizov.pro/projects/implicitbio/ для дальнейшего тестирования и отладки.

4. Отладка и тестирование системы

С помощью функции «Приватное тестирование» модуля *ImplicitBio DemoWeb* производится сбор пользовательских данных для дальнейшой отладки системы *ImplicitBio*. В эксперименте принимают участие 10 человек в возрасте от 23 до 35 лет разного пола и разной профессиональной деятельностью (в т.ч. не связанной напрямую с работой на компьютере). Каждый пользователь регистрируется с уникальным логином и паролем, на которые накладываются следующие ограничения: логин должен быть длиннее 6 символов; пароль должен быть длиннее 8 символов и содержать буквы и цифры. Подобные ограничения обычно присутствуют в веб-приложениях, а также они способствуют более качественной аутентификации по клавиатурному почерку [16, 18]. Для сбора данных типа «Подлинный пользователь» участники эксперимента со своими данными ежедневно 1 раз в день в течение двух недель проходят сценарий «Форма логина» с помощью функции «Приватное тестирование» модуля *ImplicitBio DemoWeb*. При этом накладываются определенные ограничения. Пользователи проходят сценарий используя одно и то же аппратно-программное обеспечение (компьютер, операционная система, браузер, настройки мыши, клавиатура и мышь), поскольку смена одной из этих компонент может существенно изменить значения метрик клавиатуры и мыши [32]. Кроме того, пользователям не разрешено стирать текст (в случае опечатки они проходят сценарий заново), поскольку в этом случае будет невозможно корректно сравнить клавиатурный почерк по фиксированному тексту. Для сбора данных типа «Злоумышленник» каждый пользователь проходит сценарий в роли «злоумышленника», используя учетные данные одного из других участников эксперимента («жертвы»), причем делает это последовательно 5 раз и используя аппаратно-программное обеспечение «жертвы».

Используя такие экспериментальные данные можно отладить поведенческий профиль (например, убрать из него нерепрезентативные метрики), скорретировать значения коэффициентов пороговой разности успеха (которые по умолчанию для каждой метрики были выбраны равными 0,15) и получить значения качества разработанной системы - коэффициента ложного принятия (FAR) и коэффициента ложного отказа (FRR).

4.1. Оценка репрезентативности метрик

Несмотря на то, что поведенческие биометрики были выбраны исходя из предыдущих исследований по тематике, некторые из них могут являться нерепрезентативными в рассматриваемом случае статической аутентификации, т.е. иметь непозволительно широкий разброс при их рассмотрении в контексте кокнертного элемента пользовательского интерфейса. Для идентификации таких метрик рассмотрим отклонения метрик с экспериментальных данных «Подлинный пользователь». Если независимо от пользователя найдутся метрики с недопустимо большими отклонениями, то такие метрики можно считать нерепрезентативными и исключить их из поведенческого профиля для улучшения качества аутентификации.

Рассмотрим анализ отклонений метрик с данных конкретного пользователя *Person1*. Сырые данные участника эксперимента типа «Подлинный пользователь» выгружаются с БД, на их основе создаются поведенческие профили и производятся необходимые преобразования, после чего подготовленные данные экспортируются в файл формата *JSON*. Статистический анализ данных здесь и далее происходит в среде RStudio с использованием языка программирования R.

Для метрик *delayBeforeClick*, *linearAngle*, *avgSpeed* и *avgAcceleration* формируются соответственные таблицы *clicks*, *angles*, *speeds* и *accelerations* (Рисунок 16), каждая из которых содержит значения одной метрики для трех

элементов: поля ввода логина (*login*), пароля (*password*) и кнопки (*submitButton*).

clicks | angles | speeds | accelerations

Filter

d.components.login.enterToElement.avgSpeed	d.components.password.enterToElement.avgSpeed	d.components.submitButton.enterToElement.avgSpeed
0.4613001	0.18578745	0.15569717
0.4927426	0.18062973	0.16610496
0.5386865	0.22496554	0.16713309
0.5601737	0.18069352	0.15125970
0.4085269	0.20197866	0.12348824
0.4803654	0.22932537	0.16588212
0.6953761	0.21249626	0.15136628
0.6136272	0.20985073	0.14386794
0.6976066	0.17359013	0.12543850
0.6065771	0.20849430	0.24413828
0.4804409	0.30458885	0.17574894
0.6365829	0.04861715	0.12566922
0.4635976	0.23960758	0.23801244
0.3176307	0.09185500	0.06895294

Рисунок 16. Вид таблицы *speeds*

(средняя скорость движения мыши к элементу) в среде RStudio

Для каждой таблицы производится построение диаграммы размахов (“ящики с усами”) для визуальной оценки разброса значений метрик [48]. Рассмотрим диаграмму размахов на примере таблицы *speeds* (Рисунок 17).

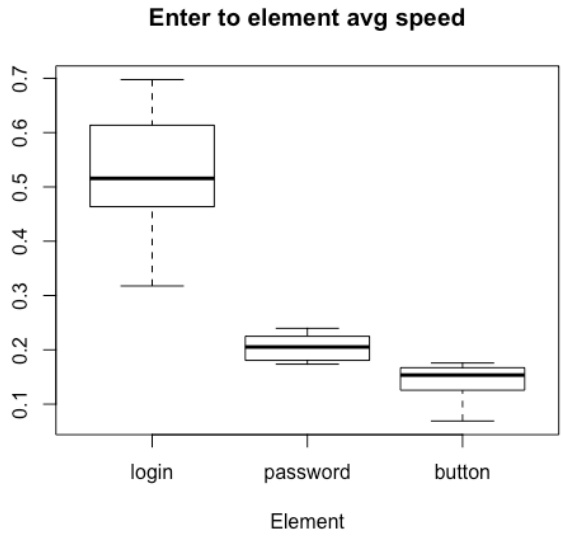


Рисунок 17. Диаграмма размахов метрики *avgSpeed* для *Person1*

Каждой колонке соответствует прямоугольник с простирающимися от него “усами”. Жирная линия внутри прямоугольника соответствует медианному значению, а сами границы – интерквартильному размаху (ИКР).

Верхний "ус" простирается от верхней границы "ящика" до наибольшего выборочного значения, находящегося в пределах расстояния 1.5 x ИКР от этой границы. Аналогично, нижний "ус" простирается от нижней границы "ящика" до наименьшего выборочного значения, находящегося в пределах расстояния 1.5 x ИКР от этой границы. Также, на графике могут присутствовать круги, которые обозначают выбросы. По диаграмме размахов метрики *avgSpeed* (Рисунок 17) мы видим, что данная метрика для пользователя *Person1* не содержит ни одного выброса. Отдельно стоит отметить, что медианное значения скорости для первого элемента (поле логина) выше более чем в 2 раза, чем у двух других. Важно отметить, что если бы метрика скорости использовалась без привязки к конкретным элементам интерфейса, ее разброс был бы более значительным, что ухудшило бы качество аутентификации. Диаграммы размахов для остальных метрик представлены в Приложении Ж.

Далее для каждого столбца таблицы (элемента интерфейса) вычисляется относительное отклонение, определяемое как отношение среднеквадратичного отклонения к среднему и выраженное в процентах, при этом «выбросы» не учитываются. Для составных метрик клавиатуры, значениями которых является массив чисел, вычисляется среднее из относительных отклонений для каждого числа. Исходный код на языке R для анализа данных одного пользователя представлен в Приложении Е. Для простоты Таблица 3 представляет вычисленные значения для двух пользователей, поскольку общая тенденция по отклонениям между пользователями одинакова. Выделенные в таблице метрики *angle* и *delayBeforeClick* имеют сильно отличающиеся и довольно большие значения средних отклонений в зависимости от элемента для всех пользователей. Таким образом, данные метрики считаются неприменимыми для использования при аутентификации пользователя по определенному сценарию и исключаются из поведенческого профиля. В то же время, остальные метрики имеют приемлемые отклонения и могут рассматриваться далее.

Таблица 3. Относительные отклонения абсолютных значений метрик для пользователей *Person1* и *Person2*.

Метрика	Относительное отклонение по элементу, %					
	login		*password*		*submitButton*	
	Person1	*Person2*	*Person1*	*Person2*	*Person1*	*Person2*
avgSpeed	25.13	22.16	19.32	20.03	27.77	24.83
linearAngle	**2.26**	**37.6**	**115.60**	**62.31**	**57.71**	**83.16**
delayBeforeClick	**72.94**	**14.42**	**86.36**	**93.45**	**46.13**	**52.55**
avgAcceleration	5.91	9.63	16.27	9.43	25.86	19.21
dwellTimes	23.46	19.53	21.83	22.56	-	-
flightTimes	19.27	25.82	24.79	24.21	-	-

4.2. Выбор пороговой разности успеха метрик

Как указывалось ранее, каждая метрика поведенческого профиля имеет свое собственное значение порога разности успеха, которое по умолчанию для всех метрик выбрано равным 0,15. Это значение определяет допустимое для успешной аутентификации отклонение метрики от ее значения в предыдущей успешной попытки аутентификации. С одной стороны, оно должно быть достаточно малым, чтобы можно было отличить двух разных пользователей, проходящих один и тот же сценарий, т.е. приводить к уменьшению FAR системы. С другой стороны, оно должно быть достаточно большим, чтобы не выдавать отказ истинному пользователю, т.е. способствовать уменьшению FRR системы.

Для определения значений пороговой разности успеха производится анализ относительной разности метрик между последовательными записями для всех пользователей. Для каждого пользователя имеющаяся выборка из 14 записей прохождения формы (типа «Подлинный пользователь») разбивается на 13 последовательных пар (1-2, 2-3 и т.д.), для каждой из которых вычисляется отчет по схожести (*similarityReport*), содержащий относительную разность для каждой метрики (имитируется процесс аутентификации). Отчеты для всех пользователей объединяются и производится анализ отклонений

относительных разностей для каждой метрики для каждого элемента интерфейса. В Приложении 3 представлены диаграммы размахов относительной разности метрик между последовательными прохождениями сценария «Форма логина» для всех пользователей. Таблица 4 представляет значения медианы и верхнего квартиля для относительной разности каждой метрики по элементу. Эти данные позволяют скорретировать значения пороговой разности успеха для каждой метрики.

Таблица 4. Относительная разность метрик по элементам для всех пользователей и выбранное значение порога относительной разности.

Метрика	Относительная разность метрики по элементу						Выбранное значение *maxSuccessDiff*
	login		*password*		*submitButton*		
	медиана	верх. кварт.	медиана	верх. кварт.	медиана	верх. кварт.	
avgSpeed	0.14	0.21	0.12	0.20	0.22	0.41	0.25
avgAcceleration	0.16	0.24	0.14	0.22	0.23	0.33	0.3
dwellTimes	0.17	0.26	0.21	0.26	-	-	0.25
flightTimes	0.27	0.33	0.28	0.31	-	-	0.3

Для метрики *avgSpeed* значние верхнего квартиля для элементов *login* и *password* не превышает 0.22, однако оно достигает существенного 0.41 для верхнего квартиля элемента *submitButton*. Существенная разница в относительных разностях метрики между элементами ввода и кнопки говорит о необходимости учитывать эту метрику для кнопки с другим пороговым коэффициентом, либо не учитывать вовсе ввиду его большого значения. На данный момент для метрики *avgSpeed* в качестве порогового (*maxSuccessDiff*) выбрано значение 0.25.

Верхний квартиль метрики *avgAcceleration* для разных элементов расположен от 0.16 до 0.33, значение пороговой разности выбрано равным 0.3. Для метрики *dwellTimes* значение выбрано равным 0.25, а для метрики *flightTimes* - 0.3.

Таким образом, на основании анализа данных двухнедельного эксперимента с 10 пользователями из поведенческого профиля были

исключены метрики *linearAngle* и *delayBeforeClick*, а для других метрик, изначально заданный пороговый коэффициент увеличился с 0.15 до 0.3 и 0.25.

4.3. Оценка качества системы

Традиционно параметрами качества системы аутентификации являются упомянутые ранее FAR и FRR. Чем ниже значение каждого из этих коэффицентов, тем более качественной считается система.

Коэффициент FRR характеризует вероятность системы выдавать отказ подлинному пользователю и равен отношению количества отказов подлинному пользователю к общему количеству попыток входа, выраженному в процентах. Для его вычисления используются данные из эксперимента «Подлинный пользователь»: для каждой записи каждого пользователя начиная со второй вычисляется реузльтат аутентификации между текущей записью и последней успешно аутентифицированной (первая запись считается подлинной). В результате для каждого пользователя формируется таблица подобная таблице 4, содержащая пару индексов сравниваемых записей и значения корневых *successCount* и *isSuccess* из отчета схожести поведенческих профилей. Вычсиленный коэффициент FRR по 130 результатам аутентификации подлинных пользователей составил 6.15%, со средним *successCount* = 2.

Таблица 5. Результаты биометрической аутентификации пользователя *Person1* по форме «Форма логина» в течечние 14 дней.

Индексы записей	*successCount*	*isSuccess*
1-0	6	TRUE
2-1	6	TRUE
3-2	6	TRUE
4-3	0	TRUE
5-4	0	TRUE
6-5	2	TRUE
7-6	2	TRUE
8-7	4	TRUE
9-8	0	TRUE
10-9	0	TRUE
11-10	0	TRUE
12-11	0	TRUE
13-12	4	TRUE
14-13	-2	FALSE

Коэффициент FAR харакетризует вероятность системы принимать неподлинного пользователя за подлинного и рассчитывается как отношение количества ложных принятий к общему количеству попыток входа, выраженное в процентах. Используются данные эксперимента «Злоумышленник»: 50 ложных записей используются для аутентификации соответствующих пользователей по их последним подлинным записям. Данная выборка показала отсутвие принятия системой таких попыток, т.е. FAR=0% со средним *successCount* = -4. Разумеется, такое низкое значение обусловленно ограниченностью выборки и на более массовом эксперименте оно будет ненулевым. Тем не менее, на этом этапе оно позволяет принять выбранные метрики и алгоритмы их сравнения и слияния приемлемыми и пригодными для проверки на дальнейших, более массовых экспериментах.

5. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

Перед тем, как представлять программный продукт на рынке информационных систем, необходимо оценить разработку с финансовой точки зрения и определить эффективность разработки и востребованность проведенного исследования. Для этого необходимо решить следующие задачи: определить цели проекта и требования к ним, провести анализ конкурентоспособности веб-сервисов, SWOT-анализ разрабатываемого программного продукта, оценить готовность продукта к коммерциализации, осуществить планирование работ, рассчитать смету затрат, оценить риски и предложить мероприятия по их минимизации, а также определить потенциальный эффект.

Разрабатываемый в данной работе программный комплекс выступает в качестве дополнительного слоя безопасности сторонних веб-приложений, существенно повышая их защищенность от взлома или кражи аккаунтов. Также он может быть использован при двухфакторной аутентификации вместо традиционных SMS и Email: в этом случае опыт пользователя будет существенно улучшен, поскольку ему не нужно будет отвлекаться на получение дополнительного кода по SMS или Email. Кроме того, использование такого способа аутентификации в веб-приложениях, зарабатывающих на платных аккаунтах, позволит выявить использование платного аккаунта несколькими людьми, что поможет существенно увеличить прибыль веб-приложения.

Потенциальными потребителями являются веб-приложения, оперирующие с ценной пользовательской информацией или платными услугами, например, приложение онлайн-банкинга или сервис для прослушивания музыки с платной подпиской.

5.1. Предпроектный анализ

5.1.1. Анализ конкурентных технических решений

Детальный анализ конкурирующих разработок, существующих на рынке, необходимо проводить систематически, поскольку рынки пребывают в постоянном движении. Такой анализ помогает вносить коррективы в научное исследование, чтобы успешнее противостоять своим соперникам. Важно реалистично оценить сильные и слабые стороны разработок конкурентов. Наиболее близкими конкурентами являются веб-сервисы зарубежных компаний KeyTrack [49] и BehavioSec [50], на российском рынке подобных веб-сервисов не выявлено.

KeyTrack – это веб-сервис, предоставляющий статическую поведенческую аутентификацию только по динамике набора текста. Система может работать в двух режимах: «усиление пароля» и «произвольный текст». Статическая аутентификация позволяет мгновенно верифицировать пользователя, однако применение системы ограничено только полями ввода и определенными пользовательскими действиями [51].

BehavioSec – это веб-сервис, предоставляющий непрерывную поведенческую аутентификацию в режиме реального времени с помощью анализа событий клавиатуры и мыши. Непрерывная аутентификация позволяет проводить аутентификацию произвольных действий пользователя, однако системе необходимо определенное время для срабатывания [50].

Разрабатываемый в рамках данной работы веб-сервис ImplicitBio использует оригинальный подход для получения и сравнения поведенческих характеристик, который позволяет системе использовать преимущества непрерывной и статической аутентификации. Кроме того, в связи с отсутствием подобных отечественных компаний, сервис имеет большой потенциал на российском рынке, в связи с чем стоимость сервиса будет существенно меньше чем у компаний-конкурентов, которые ориентированы

на европейский и американский рынки. В таблице 6 приведен анализ конкурентных технических решений.

Таблица 6. Оценочная карта сравнения конкурентных веб-сервисов

Критерий оценки	Вес критерия	Баллы			Конкурентоспособность по отдельным критериям		
		$Б_I$	$Б_B$	$Б_K$	$К_I$	$К_B$	$К_K$
Эффективность аутентификации	0.3	4	4	1	1.2	1.2	0.3
Аутентификация произвольных действий	0.2	5	3	5	1	0.6	1
Время срабатывания	0.2	3	5	2	0.6	1	0.4
Количество компонент аутентификации	0.2	5	3	4	1	0.6	0.8
Цена	0.1	5	5	2	0.5	0.5	0.2
Конкурентоспособность веб-сервиса					**4.3**	**3.9**	**2.7**

В таблице 6 индекс «I» соответствует ImplicitBio, индекс «B» – BehavioSec, индекс «K» – KeyTrack. Анализ конкурентоспособности показал, что потенциально разрабатываемый программный комплекс превосходит своих конкурентов и имеет достаточно неплохие шансы для выхода и занятия высокой позиции на рынке.

5.1.2. SWOT-анализ

SWOT-анализ заключается в выявлении сильных и слабых сторон проекта, возможностей для дальнейшего развития и угроз существованию и развитию; направлен на исследование внутренней и внешней среды проекта. Составим итоговую матрицу SWOT-анализа, представленную в таблице

Таблица 7.

Таблица 7. Матрица SWOT-анализа

	Сильные стороны: С1. Более низкая стоимость сервиса по сравнению с конкурентами; С2. Новый и эффективный способ дополнительной аутентификации; С3. Аутентификация произвольных действий;	Слабые стороны: Сл1. Отсутствие тестовой среды для отладки системы на большом количестве пользователей; Сл2. Отсутствие минимального рабочего продукта; Сл3. Отсутствие репутации на рынке.
Возможности: В1. Отсутствие конкурентов на отечественном рынке В2. Повсеместное внедрение поведенческой аутентификации; В3. Использование инфраструктуры ОЭЗ ТВТ Томск, инновационной инфраструктуры ТПУ; В4. Повышение стоимости конкурентных разработок.	Широкая область потребителей вместе с более низкой стоимостью и более эффективной защитой по сравнению с конкурентами позволят легко найти первых заказчиков. Использование инфраструктуры ОЭЗ ТВТ Томск позволит разработать минимальный рабочий продукт с наименьшим привлечением средств.	Отсутствие финансирования, тестовой среды для проведения испытаний, минимального рабочего продукта и репутации на рынке может привести к отказу стратегических предприятий от сотрудничества. Поэтому необходимо максимально использовать возможности инновационной структуры ТПУ, ОЭЗ ТВТ Томск и гранты.
Угрозы: У1. Отсутствие финансирования У2. Ограничения на экспорт продукта в связи с внешней политикой (санкциями); У3. Снижение спроса из-за высокой конкуренции;	При большом количестве конкурентов могут возникнуть трудности по внедрению продукта. В условиях нынешней политической ситуации, возможны трудности с продвижением продукта на зарубежный рынок.	При недостаточном финансировании будет сложно создать качественный и надежный сервис, а также разработать маркетинговую стратегию. Это приведёт к снижению спроса, так как разработки конкурентов могут стать более привлекательными.

Основной сильной стороной проекта является оригинальный метод, повышающий качество аутентификации. Вместе с более низкой стоимостью, а также фактом отсутствия подобных сервисов на отечественном рынке, проект имеет хорошие финансово-экономические возможности. Основной

угрозой является отсутствие финансирования, для предотвращения которой необходимо подготовить минимальный рабочий продукт и максимально использовать возможности инновационной структуры ТПУ, ОЭЗ ТВТ Томск и гранты.

5.1.3. Метод коммерциализации и оценка коммерческой готовности проекта

Наиболее подходящим методом коммерциализации результатов данной работы является организация собственного предприятия, предоставляющего разработанный сервис конечным потребителям. Такой способ коммерциализации позволит использовать конкурентное преимущество (оригинальные технические решения) и достигнуть максимального коммерческого эффекта для дальнейшего развития и улучшения системы.

Для оценки степени готовности проекта к коммерциализации заполняется Таблица 8 [51]. При оценке степени проработанности научного проекта 1 балл означает не проработанность проекта, 2 балла – слабую проработанность, 3 балла – выполнено, но в качестве не уверен, 4 балла – выполнено качественно, 5 баллов – имеется положительное заключение независимого эксперта. Для оценки уровня имеющихся знаний у разработчика система баллов принимает следующий вид: 1 означает не знаком или мало знаю, 2 – в объеме теоретических знаний, 3 – знаю теорию и практические примеры применения, 4 – знаю теорию и самостоятельно выполняю, 5 – знаю теорию, выполняю и могу консультировать.

Таблица 8. Оценка степени готовности научного проекта к коммерциализации

No п/п	Наименование	Степень проработанности научного проекта	Уровень имеющихся знаний у разработчика
1.	Определен имеющийся научно-технический задел	4	3

2.	Определены перспективные направления коммерциализации научно- технического задела	4	3
3.	Определены отрасли и технологии (товары, услуги) для предложения на рынке	4	3
4.	Определена товарная форма научно-технического задела для представления на рынок	2	2
5.	Определены авторы и осуществлена охрана их прав	1	2
6.	Проведена оценка стоимости интеллектуальной собственности	1	1
7.	Проведены маркетинговые исследования рынков сбыта	2	2
8.	Разработан бизнес-план коммерциализации научной разработки	1	2
9.	Определены пути продвижения научной разработки на рынок	1	2
10.	Разработана стратегия (форма) реализации научной разработки	3	2
11.	Проработаны вопросы международного сотрудничества и выхода на зарубежный рынок	1	2
12.	Проработаны вопросы использования услуг инфраструктуры поддержки, получения льгот	1	1
13.	Проработаны вопросы финансирования коммерциализации научной разработки	1	1
14.	Имеется команда для коммерциализации научной разработки	1	1
15.	Проработан механизм реализации научного проекта	3	4
	ИТОГО БАЛЛОВ	30	31

Суммарные значения по критериям таблицы говорят о средней перспективности научной разработки и степени разработчика к ее реализации. В целом это связано с ранним этапом исследований и малой проработкой стратегии выхода на рынок на этом этапе.

5.2. Инициация проекта

В данном разделе приводится информация о заинтересованных сторонах проекта, цели проекта и критериях достижения целей. Таблица 9 описывает заинтересованные стороны проекта. Таблица 10 описывает цель и результаты проекта.

Таблица 9. Заинтересованные стороны проекта

Заинтересованные стороны проекта	**Ожидания заинтересованных сторон**
Отделение информационных технологий ТПУ	Научные публикации Защита магистерской диссертации
Общественность	Появление на российском рынке сервиса по поведенческой аутентификации

Таблица 10. Цели и результат проекта

Цель проекта	Разработка программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях
Ожидаемые результаты проекта	1. Новый подход измерению и слиянию биометрических характеристик при мультимодальной поведенческой аутентификации 2. Новый IT-продукт, предоставляющий сервис мультимодальной аутентификации.
Критерии приемки результатов проекта	1. Опубликованы статьи с оригинальными научными идеями/результатами 2. Разработан IT-продукт, предоставляющий сервис мультимодальной аутентификации, доступно публичное демо работы сервиса.

Таблица 11 представляет оценку цели проекта с помощью SMART-теста.

Таблица 11. Smart-анализ целей проекта

Обозначение	Перевод	Комментарий относительно цели проекта
S	Конкретность	IT-продукт, предоставляющий сервис мультимодальной аутентификации.
M	Измеримость	Поставленная цель измеряется в наличии/отсутствии программного комплекса.
A	Достижимость	Имеющихся временных и интеллектуальных ресурсов достаточно для достижения цели.
R	Актуальность	Отсутствие отечественных разработок и необходимость усиления безопасности в веб-приложениях
T	Временные рамки	Достижение цели ограничено периодом с сентября до мая 2019 года.

Таблица 12 представляет рабочую группу проекта.

Таблица 12. Рабочая группа проекта

№ п/п	ФИО, основное место работы, должность	Роль в проекте	Функции	Трудо-затраты, раб. дни.
1	Савельев Алексей Олегович, ТПУ, доцент	руководитель	Координирует деятельность исполнителя	16
2	Газизов Александр Тальгатович, ТПУ, студент	исполнитель	Выполняет работы по проекту	148

Таким образом, представленные в данном разделе таблицы дают исчерпывающую информацию для инициации проекта. Сформулированная цель проекта проверена SMART-анализом, а также описана рабочая группа проекта. Наиболее значимым планируемым результатом проекта является появление первого на отечественном рынке IT-продукта, предоставляющего сервис мультимодальной аутентификации.

5.3. Планирование проектных работ

5.3.1. План проекта

Планирование комплекса предполагаемых работ осуществляется в следующем порядке:

– определение структуры работ в рамках научного исследования;

– определение участников каждой работы;

– установление продолжительности работ;

– построение графика научных исследований.

Рабочая группа, выполняющая научные исследования, состоит из двух человек: научного руководителя и студента – непосредственного исполнителя.

Трудовые затраты в большинстве случаев образуют основную часть стоимости разработки, поэтому важным моментом является определение трудоемкости работ каждого из участников научного исследования.

Трудоемкость выполнения научного исследования оценивается экспертным путем в человеко-днях и носит вероятностный характер, т.к. зависит от множества трудно учитываемых факторов. Для определения ожидаемого (среднего) значения трудоемкости $t_{ожi}$ используется следующая формула:

$$t_{\text{ожі}} = \frac{3t_{\min i} + 2t_{\max i}}{5},$$

где $t_{ожi}$ – ожидаемая трудоемкость выполнения *i*-ой работы чел.-дн.;

$t_{\min i}$ – минимально возможная трудоемкость выполнения заданной *i*-ой работы (оптимистическая оценка: в предположении наиболее благоприятного стечения обстоятельств), чел.-дн.;

$t_{\max i}$ – максимально возможная трудоемкость выполнения заданной *i*-ой работы (пессимистическая оценка: в предположении наиболее неблагоприятного стечения обстоятельств), чел.-дн.

Исходя из ожидаемой трудоемкости работ, определяется продолжительность каждой работы в рабочих днях $T_р$. Длительность каждого из этапов работ из рабочих дней переводится в календарные дни. Для этого используется следующая формула:

$$T_{кi} = T_{рi} \cdot k_{кал},$$

где $T_{кi}$– продолжительность выполнения *i*-й работы в календарных днях;

$T_{рi}$ – продолжительность выполнения *i*-й работы в рабочих днях;

$k_{кал}$– коэффициент календарности.

Коэффициент календарности определяется по следующей формуле:

$$k_{кал} = \frac{T_{кал}}{T_{кал} - T_{вых} - T_{пр}},$$

где $T_{кал}$ – количество календарных дней в году;

$T_{вых}$ – количество выходных дней в году;

$T_{пр}$ – количество праздничных дней в году.

Согласно производственному календарю (для 6-дневной рабочей недели) в 2019 году 365 календарных дней, 299 рабочих дней, 66 выходных/праздничных дней и $k_{кал}$= 1,22. Рассчитанные значения в календарных днях по каждой работе $T_{кi}$ округляются до целого числа.

Временны́е показатели проведения научного исследования сведены в таблице 13. На ее основании разработан календарный план-график проведения работ студентом (Таблица 14).

Таблица 13. Временны́е показатели проведения научного исследования: Исп. 1 – Александр Газизов, Исп. 2 – научный руководитель Алексей Олегович Савельев

Название работы	**Трудоёмкость работ**						**Длительность работ в рабочих днях T_{pi}**		**Длительность работ в календарных днях T_{ki}**	
	t_{min}, чел-дни		t_{max}, чел-дни		$t_{ожі}$, чел-дни					
	Исп.1	Исп.2	Исп.1	Исп.2	Исп.1	Исп.2	Исп.1	Исп.2	Исп.1	Исп.2
Выбор направления научного исследования	5	1	10	1	7	1	7	1	9	2
Составление и утверждение технического задания	5	1	10	1	7	1	7	1	9	2
Обзор литературы	14	0	18	0	15.6	0	16	0	20	0
Разработка архитектуры программного комплекса	5	1	10	1	7	1	7	1	9	2
Разработка модуля ImplicitBio Recorder	5	1	10	1	7	1	7	1	9	2
Тестирование модуля ImplicitBio Recorder	5	1	10	2	7	1.4	7	2	9	3
Проектирование модуля ImplicitBio Server	5	1	10	1	7	1	7	1	9	2
Реализация модуля ImplicitBio Server	10	1	18	1	13.2	1	14	1	18	2
Тестирование модуля ImplicitBio Server	8	1	14	1	10.4	1	11	1	14	2
Разработка модуля ImplicitBio DemoWeb	10	0	20	0	14	0	14	0	18	0
Проектирование и проведение 1-го эксперимента	10	1	20	1	14	1	14	1	18	2
Анализ результатов эксперимента и корректировка системы	5	1	10	1	7	1	7	1	9	2
Проектирование и проведение 2-го эксперимента	4	1	8	1	5.6	1	6	1	8	2
Анализ результатов и финальные доработки	4	1	5	1	4.4	1	5	1	7	2
Создание отчетов и документов	14	2	18	2	15.6	2	16	2	20	3
Подготовка презентации дипломного проекта	2	1	4	1	2.8	1	3	1	4	2
Итого	**111**	**15**	**195**	**16**	**144.6**	**15.4**	**148**	**16**	**190**	**30**

Таблица 14. Календарный план-график проведения работ. ■ - Исп. 1, ▨ - Исп. 2.

Название работы		Продолжительность выполнения работ																								
		сент.			окт.			нояб.			дек.			янв.			фев.			мар.			апр.			май
	T_{ki}	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
Выбор направления научного исследования	9	■	▨																							
Составление и утверждение технического задания	9		■	▨																						
Обзор литературы	20			■	■	■	▨																			
Разработка архитектуры программного комплкса	9					■	▨																			
Разработка модуля ImplicitBio Recorder	9						■	▨																		
Тестирование модуля ImplicitBio Recorder	9							■	▨																	
Проектирование модуля ImplicitBio Server	9								■	▨																
Реализация модуля ImplicitBio Server	18									■	■	■	▨													
Тестирование модуля ImplicitBio Server	14											■	▨				■	■	▨							
Разработка модуля ImplicitBio DemoWeb	18																■	■	■	■	■	▨				
Проектирование и проведение 1-го эксперимента	18																			■	■	■	■	■	▨	
Анализ результатов эксперимента и корректировка системы	9																						■	▨		
Проектирование и проведение 2-го эксперимента	8																							■	▨	
Анализ результатов и финальные доработки	7																								■	▨
Создание отчетов и документов	20																								■	■
Подготовка презентации дипломного проекта	4																									■

5.3.2. Бюджет научно-технического исследования

В ходе выполнения работы не приобретались какие-либо специальные материалы и комплектующие. Были закуплены канцелярские принадлежности на сумму 500 рублей.

5.3.2.1. Амортизационные отчисления

В ходе работы использовалось личное оборудование студента, ноутбук Acer стоимостью 40000 руб. Принимаем срок полезного использования равным 3 года (машины офисные, код 330.28.23.23), планируем использовать ноутбук для выполнения работы в течение 9 месяцев. Рассчитаем его амортизацию:

- норма амортизации:

$$Ан = \frac{1}{n} * 100\% = \frac{1}{3} * 100\% = 33{,}33\%$$

- годовые амортизационные отчисления:

$$Аг = 40000 * 0{,}33 = 13200 \text{ рублей}$$

- ежемесячные амортизационные отчисления:

$$Ам = \frac{13200}{12} = 1100 \text{ рублей}$$

- итоговая сумма амортизации основных средств:

$$А = 1100 * 9 = 9900 \text{ рублей}$$

5.3.2.2. Основная заработная плата исполнителей темы

В качестве оклада инженера принимаем оклад равный 21760 руб. Оклад руководителя равна 33664 руб.

Заработная плата основная рассчитывается по формуле

$$Зосн = Здн \times Тр \times (1 + Кпр + Кд) \times Кр, \text{ где}$$

Здн – среднедневная заработная плата, руб.

Кпр – премиальный коэффициент, принят равным 0,3;

Кд – коэффициент доплат и надбавок, принят равным 0,2;

Кр – районный коэффициент (для Томска равен 1,3);

Тр – продолжительность работ, выполняемых работником, раб. дни (берется из таблицы 13).

Среднедневная заработная плата рассчитывается по формуле

$$Здн = \frac{Зм \times М}{F_д}, \text{ где}$$

Зм – оклад работника за месяц, руб.

М – количество месяцев работы без отпуска в течение года (при отпуске в 48 раб. дней М=10,4 месяца, 6-дневная неделя)

Fд – действительный годовой фонд рабочего времени персонала (календарные дни за вычетом нерабочих дней, равный 365 – 66 – 56 = 243)

Тогда для студента

$$Здн\ ст = \frac{Зм \times М}{F_д} = \frac{21760 \times 10{,}4}{243} = 931{,}29 \text{ руб.}$$

Для научного руководителя

$$Здн\ рук = \frac{Зм \times М}{F_д} = \frac{33664 \times 10{,}4}{243} = 1440{,}76 \text{ руб.}$$

Таблица 15 представляет расчет основной заработной платы.

Таблица 15. Расчет основной заработной платы

Исполнители	Здн, руб.	Кпр	Кд	Кр	Тр	Зосн, руб
Инженер	931,29	0,3	0,2	1,3	148	268770
Научный руководитель	1440,76	0,3	0,2	1,3	16	44951
Итого:						**313721**

5.3.2.3. Формирование сметы затрат проекта

К вышеуказанным затратам добавляется дополнительная заработная плата исполнителей (15% от основной заработной платы), страховые отчисления (30% от заработной платы), а также накладные расходы (16% от всех расходов) [51]. Таблица 16 представляет бюджет затрат исследования. Таким образом, суммарный бюджет проекта составит 581523 руб.

Таблица 16. Смета затрат

Наименование	Сумма, руб.	Удельный вес, %
Материальные затраты	500	0.09
Затраты на амортизацию	9900	1.75
Затраты на основную заработную плату	313721	55.45
Затраты на дополнительную заработную плату	49586	8.76
Страховые взносы	114049	20.16
Накладные расходы	78040.96	13.79
Общий бюджет	565796.96	100

5.3.3. Риски проекта

Риск – это возможность наступления некоторого неблагоприятного события, влекущего за собой возникновение различного рода потерь. Таблица 17 представляет группы рисков и их описания для данного проекта.

Таблица 17. Определение рисков

№ п/п	Наименование риска	Описание риска
1	Политические	Возможны негативные изменения в государственной политике, направленные на запрет отслеживания поведения пользователей или повышение налогов для IT-компаний
2	Экономические	Изменение экономической ситуации, например, укрепление курса рубля может привести к незначительной разнице в стоимости сервиса по сравнению с конкурентами.
3	Социальные	Исполнители проекта могут стать временно нетрудоспособными по состоянию здоровья.
4	Экологические	Вероятность возникновения отрицательных изменений в окружающей природной среде или отдалённых неблагоприятных последствий этих изменений, возникающих вследствие негативного воздействия на окружающую среду.
5	Технологические	Сбои в программной обеспечении, утрата базы данных
6	Финансовые	Риски, связанные с вероятностью потерь финансовых ресурсов.
7	Организационные	Риски, связанные с внутренней организацией работы исполнителей.
8	Маркетинговые	Риски, связанные с маркетинговой стратегией проекта
9	Кадровые	Риски в процессе принятия и реализации кадровых решений

10	Технические	Являются следствиями технических неисправностей, некачественных ремонтов, физическим и моральным износом оборудования.

Таблица 18 представляет реестр рисков для проекта и включает: вероятность риска, уровень потерь, а также мероприятия по снижению риска. Ячейки вероятности и уровня потерь риска имеют цветовую дифференциацию:

Красная область – высокий риск;

Желтая область – существенный риск;

Синяя область – умеренный риск;

Зеленая область – незначительный риск.

Таблица 18. Реестр рисков

№ п/п	Наименование риска	Оценка вероятности риска (низкая, средняя, высокая)	Оценка уровня потерь (низкий, средний, высокий)	Мероприятия по снижению риска
1	Политические	низкая	низкий	Следить за государственной политикой в IT-сфере, проявлять активную гражданскую позицию
2	Экономические	низкая	низкий	Следить за экономической ситуацией и корректировать стоимость продукта
3	Социальные	низкая	низкий	-
4	Экологические	низкая	нулевой	-
5	Технологические	средняя	высокий	Привлекать внешних экспертов для аудита исходного кода программ; писать автоматические тесты для программ; проводить тщательное тестирование новых версий перед выходом в свет
6	Финансовые	средняя	средний	Иметь в виду текущие и наиболее вероятные будущие финансовые показатели при ведении проекта
7	Организационные	нулевая	низкий	-
8	Маркетинговые	средняя	высокий	Уделить должное время разработке маркетинговой стратегии, получить внешнюю экспертизу
9	Кадровые	нулевая	низкий	-
10	Технические	низкая	средний	Уделить должное внимание инфраструктуре проекта: выбрать качественный и надежный сервер

Анализ рисков проекта показал, что наиболее существенными являются технологические, финансовые и маркетинговые риски. Для успеха проекта необходимо в первую очередь сконцентрироваться на мероприятиях (Таблица 18), направленных на снижение этих рисков.

5.4. Описание потенциального эффекта

В данном разделе разрабатываемый программный комплекс был оценен с финансовой точки зрения. Определены потенциальные потребители разработки – это веб-приложения, оперирующие с ценной пользовательской информацией или платными услугами, например, приложение онлайн-банкинга или сервис для прослушивания музыки с платной подпиской. Проведен анализ конкурентных технических решений, показавший, что разрабатываемый продукт превосходит своих конкурентов по таким праметрам как «эффективность аутентификации», «аутентификация произвольных действий» и «количество компонент аутентификации».

SWOT-анализ помог выявить сильные и слабые стороны разработки, которые позволили повысить ее эффективность и уменьшить давление угроз со стороны внешних факторов. Благодаря оригинальной технологии конечного продукта и отсутствию конкурентов на отечественном рынке возможен быстрый срок окупаемости проекта и устранение угроз, описанных в SWOT-анализе. При этом особое внимание следует уделить выходу продукта на рынок и его продвижению, установлению сотрудничества с крупными заказчиками. Для этого на данном этапе необходимо активное участие в конференциях, выставках и форумах, а также участие в грантах и конкурсах на получение финансирования для малых инновационных предприятий.

Также в данной главе была определена структура работ проекта и назначены ответственные исполнители. На основе этого была рассчитана трудоемкость работ и составлена диаграмма Ганта (график работ). Таким образом, общая длительность проектирования и разработки приложения составила 190 дней.

Рассчитанные финансовые ресурсы, требуемые для разработки программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях, составляют порядка 565796 рублей. В эту сумму включены материальные затраты, затраты на основную заработную

плату, на дополнительную заработную плату, а также накладные расходы и отчисления во внебюджетные фонды. Учитывая срок выполнения проекта (9 месяцев) и количество участников (2 человека) эта цифра является приемлемой.

6. Социальная ответственность

В этом разделе рассматриваются особенности организации рабочего места специалиста, осуществляющего работу по созданию программного комплекса для неявной мультимодальной поведенческой аутентификации в веб-приложениях. Предполагается, что работа осуществляется в закрытом, отапливаемом и вентилируемом помещении, на рабочем месте, оснащенном персональным компьютером.

Далее будут рассмотрены факторы рабочей зоны и рабочего места, влияющие на состояние сотрудника, а также влияние проектной деятельности на состояние окружающей среды.

6.1.Правовые и организационные вопросы обеспечения безопасности

Предъявляемые требования к расположению и компоновке рабочего места:

«Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах (680÷ 800) мм, при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм [53].

Модульными размерами рабочей поверхности стола для ПК, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм [53].

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450мм и на уровне вытянутых ног – не менее 650 мм [53].

Конструкция рабочего стула должна обеспечивать:

– ширину и глубину поверхности сиденья не менее 400 мм;

– поверхность сиденья с закругленным передним краем;

– регулировку высоты поверхности сиденья в пределах (400 ÷ 550) мм и углам наклона вперед до 15 град, и назад до 5 град.;

– высоту опорной поверхности спинки (300±20) мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости –400 мм;

– угол наклона спинки в вертикальной плоскости в пределах ±30 градусов;

– регулировку расстояния спинки от переднего края сиденья в пределах (260÷ 400) мм;

– стационарные или съемные подлокотники длиной не менее 250мм и шириной – (50÷ 70) мм;

– регулировку подлокотников по высоте над сиденьем в пределах(230±30) мм и внутреннего расстояния между подлокотниками в пределах (350÷ 500) мм [53].

Рабочее место пользователя ПК следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм [53].

Клавиатуру следует располагать на поверхности стола на расстоянии (100 ÷ 300) мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы [53].

Экран видеомонитора должен находиться от глаз пользователя на расстоянии (600÷ 700 мм), но не ближе 500 мм [53].

Рекомендуется работать в помещении, где окна выходят на север или северо-восток. Местное освещение не должно создавать блики на поверхности экрана дисплея. Недопустим яркий не рассеянный верхний свет (с потолка). Сдерживать поток избыточного света от окон следует с помощью жалюзи (или тканевых штор); чистота обязательна при работе за компьютером. Влажную уборку помещения следует проводить ежедневно. Недопустима запыленность

воздуха, пола, рабочей поверхности стола и техники. Помещение должно быть оборудовано системами вентиляции, кондиционирования и отопления.

6.2. Производственная безопасность

Таблица 19. Опасные и вредные факторы при выполнении работ по разработке программного комплекса.

Источник фактора, наименование видов работ	Факторы (по ГОСТ 12.0.003-74)		Нормативные документы
	Вредные	Опасные	
1. Работа за персональным компьютером. 2. Работа с оборудованием в помещении	1. Недостаточная освещённость рабочей зоны: отсутствие или недостаток естественного света; 2. Повышенный уровень шума; 3. Повышенный уровень электромагнитных излучений; 4. Повышенная или пониженная влажность воздуха	1. Электрический ток	1. СП 52.13330.2011 Свод правил. Естественное и искусственное освещение. [52] 2. СанПиН 2.2.2/2.4.1340 – 03. Санитарно-эпидемиологические правила и нормативы «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». [53] 3. СН 2.2.4/2.1.8.562 – 96. Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории застройки. [54] 4. ГОСТ 12.1.038-82 ССБТ. Электробезопасность. Предельно допустимые уровни напряжений прикосновения и токов. [55] 5. СанПиН 2.2.4.548 – 96. Гигиенические требования к микроклимату производственных помещений. [56]

6.2.1. Недостаточная освещённость рабочей зоны; отсутствие или недостаток естественного света

Освещение рабочего места специалиста складывается из естественного и искусственного освещения. Естественное освещение достигается установкой оконных проемов с коэффициентом естественного освещения КЕО не ниже 1,2 % в зонах с устойчивым снежным покровом и не ниже 1,5 % на остальной территории [62].

Нормируемые показатели естественного, искусственного и совмещенного освещения в соответствии с СанПиН 2.2.1/2.1.1.1278-03 указаны в таблице 20 [63].

Таблица 20. Нормируемые показатели естественного, искусственного и совмещенного освещения в соответствии с СанПиН 2.2.1/2.1.1.1278-03

Помещения	Рабочая поверхность и плоскость нормирования КЕО и освещенности (Г – горизонтальная, В – вертикальная) и высота плоскости над полом, м	Естественное освещение		Совмещенное освещение		Искусственное освещение				
		КЕО e_н, %		КЕО e_н, %		Освещенность, лк				
		При верхнем или комбинированном освещении	При боковом освещении	При верхнем или комбинированном освещении	При боковом освещении	При комбинированном освещении		При общем освещении	Показа-тельдискомфорта, М, не более	Коэффициент пульсации освещенности, К_п, %, не более
						всего	от общего			
1	2	3	4	5	6	7	8	9	10	11
Кабинеты, рабочие комнаты, офисы	Г – 0,8	3,0	1,0	1,8	0,6	400	200	300	40	15
Помещения для работы с дисплеями и видеотерминалами, залы ЭВМ	Г – 0,8 Экран монитора: В – 1,2	3,5 -	1,2 -	2,1 -	0,7 -	500 -	300 -	400 200	15 -	10

Для искусственного освещения помещений с персональными компьютерами следует применять светильники типа ЛПО36. Допускается применять светильники прямого света, преимущественно отраженного света типа ЛПО13, ЛПО5, ЛСО4, ЛПО34, ЛПО31 с люминесцентными лампами

типа ЛБ. Допускается применение светильников местного освещения с лампами накаливания. Светильники должны располагаться линиями (прямыми или прерывающимися) так, чтобы при разном положении машин они были параллельно линии зрения пользователя. Защитный угол светильников должен быть не менее 40 градусов [63].

В утреннее и вечернее время вводится общее искусственное освещение. Основными источниками искусственного освещения являются лампы белого света ЛБ-20.

Для обеспечения нормируемых значений освещенности по СанПиН 2.2.1/2.1.1.1278-03 в помещениях для работы за ПК следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

Выполним расчет естественного освещения. Расчет производится согласно СНиП 23.05-95 «Естественное и искусственное освещение». Рабочая аудитория имеет размеры 6 х 5 х 2,5 м, в которой установлены 2 окна размером 1,6 х 2,2 м. Освещение боковое, одностороннее, выделение пыли и других аэрозолей допустимо с концентрацией не более 5 $мг/м^3$.

Зная размеры окон и их количество, можем рассчитать эквивалентную площадь световых проемов по формуле (1):

$$S_{экв} = N \cdot S_{окна} = 2 \cdot 1{,}6 \cdot 2{,}2 = 7{,}04\ м^2. \quad (1)$$

Площадь помещения найдём из размеров аудитории по формуле (2):

$$S = 6 \cdot 5 = 30\ м^2. \quad (2)$$

Далее также будут применены следующие величины [52, 63]:

а) $n_0 = 9$ – световая характеристика окна, зависящая от глубины помещения, выступа окна и соотношения длин сторон;

б) $K_{ЗД} = 1{,}2$ – коэффициент, учитывающий уменьшение КЕО от затемнения противостоящим зданием;

в) $r_1 = 3$ – коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отраженному от внутренних поверхностей;

г) t_0 – общий коэффициент светопропускания, вычисляющийся как

д) $t_0 = t_1 \cdot t_2 \cdot t_3 \cdot t_4 = 0{,}8 \cdot 0{,}6 \cdot 0{,}7 \cdot 0{,}8 = 0{,}27$, где:

t_1 – зависит от вида светопропускающего материала. Для двойного оконного стекла равен 0,8;

t_2 – зависит от вида проема. Для деревянных раздельных оконных рам равен 0,6.

t_3 – зависит от степени загрязнения светопропускающего материалаю. Для умеренного загрязнения пылью равен 0,7;

t_4 – зависит от несущих конструкций. Выбран по таблице соответствующих коэффициентов в [62] равным 0,8.

Рассчитаем фактический коэффициент естественного освещения (КЕО) по формуле (3):

$$\text{КЕО}_\text{ф} = \frac{S_\text{экв} \cdot t_\text{о} \cdot r_1 \cdot 100}{S \cdot n_\text{о} \cdot K_\text{ЗД}} = \frac{7{,}04 \cdot 0{,}27 \cdot 3 \cdot 100}{30 \cdot 9 \cdot 1{,}2} = 1{,}76. \quad (3)$$

Получили, что фактический коэффициент естественного освещения соответствует норме согласно СанПиН 2.2.1/2.1.1.1278-03 [12].

Рассчитаем фактическое искусственное освещение. На рассматриваемом рабочем месте основными источниками искусственного освещения являются лампы белого света ЛБ-20 в количестве $N = 16$ шт. Световой поток одной лампы $F = 1180$ лм. Коэффициент запаса примем равным $k = 1{,}1$, а коэффициент минимальной освещённости $z = 1{,}1$.

Найдем индекс помещения по формуле (4):

$$i = \frac{S}{h_\text{р} \cdot (\text{а} + b)}, \quad (4)$$

где:

S – площадь помещения;

а и b – длина и ширина помещения;

$h_\text{р}$ – расчетная высота, равная:

$$h_\text{р} = h - h_c - h_\text{р.п}, \quad (5)$$

где:

h – высота помещения;

$h_c = 0{,}2$ м – расстояние от перекрытия до светильника;

$h_{\text{р.п}} = 1$ м – расстояние от пола до рабочей поверхности.

Отсюда, индекс помещения равен:

$$i = \frac{S}{(h - h_c - h_{\text{р.п}}) \cdot (\text{a} + b)} = \frac{30}{(2{,}5 - 0{,}2 - 1) \cdot (6 + 5)} = 2{,}09. \qquad (6)$$

Зная индекс помещения, определим коэффициент использования светового потока по существующей таблице [55]. Коэффициент использования светового потока равен $n = 0{,}62$.

Теперь воспользуемся формулой (7) и рассчитаем фактическое искусственное освещение:

$$E = \frac{F \cdot N \cdot n}{S \cdot z \cdot k} = \frac{1180 \cdot 16 \cdot 0{,}62}{30 \cdot 1{,}1 \cdot 1{,}1} = 322{,}46 \text{ лк.} \qquad (7)$$

Таким образом, из рассчитанных данных видно, что использование имеющегося числа газоразрядных ламп достаточно для соблюдения норм искусственной освещенности на рабочем месте согласно СанПиН 2.2.1/2.1.1.1278-03 [63].

6.2.2. Повышенный уровень шума

При выполнении работ, описанных выше, специалист может оказаться под шумовым воздействием со стороны оборудования, находящегося в рабочем помещении: персональные компьютеры, печатающие устройства, оборудование поддержки микроклимата (кондиционеры, вентиляция) и прочее.

Работы, выполняемые специалистом, оцениваются как научная деятельность, конструирование и проектирование, программирование, следовательно, согласно СН2.2.4/2.1.8.562-96 эквивалентный уровень шума в рабочем помещении недолжен превышать 50дБА.

Таблица 21. Эквивалентные уровни звука для проектно-конструкторских бюро, лабораторий для теоретических работ по СН 2.2.4/2.1.8.562 – 96. [54]

Вид трудовой деятельности, рабочее место	**Эквивалентные уровни шума, дБА**
Творческая деятельность, руководящая работа с повышенными требованиями, научная деятельность, конструирование и проектирование, программирование, преподавание и обучение, врачебная деятельность. Рабочие места в помещениях дирекции, проектно-конструкторских бюро, расчетчиков, программистов вычислительных машин, в лабораториях для теоретических работ и обработки данных, приема больных в здравпунктах	50

В качестве мер по снижению шума, воздействующего на человека, в первую очередь следует использовать средства коллективной защиты. Наиболее эффективной защитой от шума, источником которого являются циркуляционные насосы программно-аппаратного комплекса, было бы создание специальных архитектурно-строительных решений на этапе проектирования рабочего места в рабочей аудитории, но так как помещение в момент строительства здания не планировалось использовать для таких целей, то единственным решением по принятию мер коллективной защиты от производственного шума является использование акустического экрана или звукоизолирующего кожуха [62].

В качестве индивидуальных средств защиты от шума специалистом могут быть использованы специальные противошумные наушники, которые обезопасят пользователя от вредного воздействия шумов и помогут сделать условия работы более комфортными [62].

6.2.3. Повышенный уровень электромагнитных излучений; повышенная напряжённость электрического поля

Источником электромагнитного поля и электромагнитных излучений на рабочем месте является компьютер, в частности экран монитора компьютера. Мощность экспозиционной дозы мягкого рентгеновского излучения в любой точке на расстоянии 0,05 м от экрана при любых положениях ПК не должна превышать 100 мкР/час [53].

Время работы на персональном компьютере по санитарным нормам не должно превышать 4 часа.

Допустимые значения параметров неионизирующих электромагнитных излучений от монитора компьютера представлены в таблице 22.

Таблица 22. Допустимые значения параметров неионизирующих электромагнитных излучений по СанПиН 2.2.2/2.4.1340 – 03. [53]

Наименование параметра	**Допустимые значения**
Напряженность электрической составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	10 В/м
Напряженность магнитной составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	0,3 А/м
Напряженность электростатического поля не должна превышать: – для взрослых пользователей	20 кВ/м

Предельно-допустимые нормы ЭМП представлены в таблице 23.

Таблица 23. Предельно допустимые нормы ЭМП по СанПиН 2.2.4.548 – 96. [56]

Напряжённость электрического поля	
в диапазоне частот 5 Гц - 2 кГц	25 В/м
в диапазоне частот 2 кГц - 400 кГц	2,5 В/м
Плотность магнитного потока	
в диапазоне частот 5 Гц - 2 кГц	250 нТл
в диапазоне частот 2 кГц - 400 кГц	25 нТл

Ряд мероприятий, позволяющих уменьшить влияние вредных факторов на работника при работе за ПК: каждый час необходимо делать перерыв, для выполнения гимнастики для глаз, а также выполнять несколько упражнений на расслабление, которые могут уменьшить напряжение, накапливающееся в мышцах при длительной работе за компьютером [53].

6.2.4. Микроклимат

Для создания благоприятных условий работы, соответствующих физиологическим потребностям человеческого организма, санитарные нормы устанавливают оптимальные и допустимые метеорологические условия в

рабочей зоне помещения [53] (табл. 24, 25). Выполняемая работа относится к категории легкая (1б).

Таблица 24. Оптимальные величины показателей микроклимата на рабочих местах производственных помещений по СанПиН 2.2.4.548-96 [56]

Период года	Температура воздуха, ^{0}C	Температура поверхностей, ^{0}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	21 - 23	20 – 24	60-40	0,1
Теплый	23-25	22-26	60-40	0,1

Таблица 25. Допустимые величины показателей микроклимата на рабочих местах производственных помещений по СанПиН 2.2.4.548-96 [56]

Период года	Температура воздуха, °C		Температура поверхностей, °C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с	
	Диапазон ниже оптимальных величин	Диапазон выше оптимальных величин			Для диапазона температур воздуха ниже оптимальных величин, не более	Для диапазона температур воздуха выше оптимальных величин, не более
Холодный	19,0 - 20,9	23,1 - 24,0	18,0 - 25,0	15 - 75	0,1	0,2
Теплый	20,0 - 21,9	24,1 - 28,0	19,0 - 29,0	15 - 75	0,1	0,3

В данном случае температура воздуха и температура поверхностей составляют 22 ^{0}C и 21 ^{0}C при относительной влажности 45 % в холодный период года; 24 ^{0}C и 23 ^{0}C при относительной влажности воздуха 50 % в теплый период года, что соответствует нормам [66].

6.2.5. Электрический ток (источник: ПК)

Токи статического электричества, наведенные в процессе работы компьютера на корпусах монитора, системного блока и клавиатуры, могут приводить к разрядам при прикосновении к этим элементам. Такие разряды опасности для человека не представляют, но могут привести к выходу из строя вышеописанного оборудования.

На рабочем месте пользователя размещены дисплей, клавиатура и системный блок. Перед началом работы следует убедиться в отсутствии

свешивающихся со стола или висящих под столом проводов электропитания, в целостности вилки и провода электропитания, в отсутствии видимых повреждений аппаратуры и рабочей мебели, в отсутствии повреждений и наличии заземления приэкранного фильтра.

Методы защиты от воздействия статического электричества:

– влажная уборка, чтобы уменьшить количество пылинок в воздухе и на предметах офиса;

– использование увлажнителей воздуха;

– защитное заземление;

– применение средств индивидуальной защиты, таких как антистатические спреи и браслеты.

Допустимый ток частотой 50 Гц при длительности воздействия более 10 секунд составляет 2 мА, а при длительности 10 секунд и менее – 6 мА. Для переменного тока эта величина соответственно равна 10 и 15 мА [55].

Методы защиты от опасности поражения электрическим током:

– электрическая изоляция токоведущих частей (сопротивление изоляции должно быть не менее 0,5 МОм);

– ограждение токоведущих частей, которые работают под напряжением;

– использование малых напряжений, например, не более 50 В;

– электрическое разделение сетей на отдельные короткие участки;

– защитное заземление и зануление;

– применение средств индивидуальной защиты, таких как плакаты и знаки безопасности, изолирующие подставки, указатели напряжения.

6.3. Экологическая безопасность

Охрана окружающей среды сводится к устранению отходов бытового мусора и отходам жизнедеятельности человека. В случае выхода из строя ПК, они списываются и отправляются на специальный склад, который при необходимости принимает меры по утилизации списанной техники и комплектующих [66].

Одним из самых распространенных источников ртутного загрязнения являются вышедшие из эксплуатации люминесцентные лампы. Каждая такая лампа, кроме стекла и алюминия, содержит около 60 мг ртути. Поэтому отслужившие свой срок люминесцентные лампы, а также другие приборы, содержащие ртуть, представляют собой опасный источник токсичных веществ [66].

Утилизация ламп предполагает передачу использованных ламп предприятиям – переработчикам, которые с помощью специального оборудования перерабатывают вредные лампы в безвредное сырье – сорбент, которое в последующем используют в качестве материала для производства, например, тротуарной плитки.

Под хранением отходов понимается временное размещение их в специально отведённых для этого местах или объектах до их утилизации [62]. Отработанные люминесцентные лампы, согласно Классификатору отходов ДК 005-96, утвержденному приказом Госстандарта № 89 от 29.02.96 г., относятся к отходам, которые сортируются и собираются отдельно, поэтому утилизация люминесцентных ламп и их хранение должны отвечать определенные требованиям.

6.4. Безопасность в чрезвычайных ситуациях

6.4.1. Пожарная безопасность

Компьютерный класс по пожарной безопасности относится к категории В, в нём находятся горючие материалы и вещества в холодном состоянии [60]. По степени огнестойкости данное помещение относится к 3-й степени огнестойкости [61]. Возможные причины пожара: перегрузка в электросети, короткое замыкание, разрушение изоляции проводников.

Для локализации или ликвидации загорания на начальной стадии используются первичные средства пожаротушения:

– огнетушащие вещества (вода, песок, земля);

– огнетушащие материалы (грубошерстные куски материи – кошмы, асбестовые полотна, металлические сетки с малыми ячейками ит. п.);

– немеханизированный ручной пожарный инструмент (багры, крюки, ломы, лопаты и т. п.);

– пожарный инвентарь (бочки и чаны с водой, пожарные ведра, ящики и песочницы с песком);

– пожарные краны на внутреннем водопроводе противопожарного водоснабжения в сборе с пожарным стволом и пожарным рукавом;

– огнетушители [62].

Первичные средства пожаротушения обычно применяют до прибытия пожарной команды.

Здание должно соответствовать требования пожарной безопасности, а именно, наличие охранно-пожарной сигнализации, плана эвакуации (рисунок 18), порошковых огнетушителей с поверенным клеймом, табличек с указанием направления к запасному (эвакуационному) выходу.

Углекислотные огнетушители ОУ-3, ОУ-5 предназначены для тушения загораний веществ, горение которых не может происходить без доступа воздуха, загораний электроустановок, находящихся под напряжением не более 1000В, жидких и газообразных веществ (класс В, С).

Огнетушители не предназначены для тушения загорания веществ, горение которых может происходить без доступа воздуха (алюминий, магний и их сплавы, натрий, калий), такими огнетушителями нельзя тушить дерево.

На рисунке 18 представлен план эвакуации при пожаре и других ЧС.

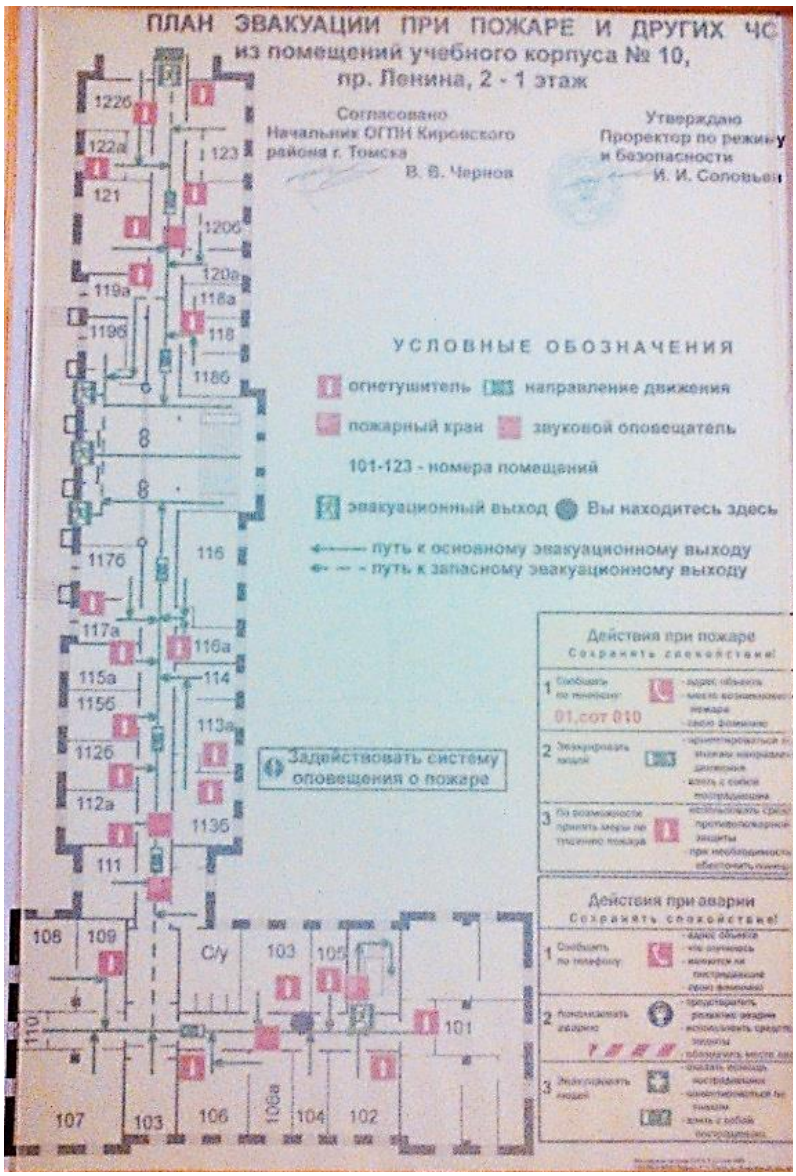


Рисунок 18. План эвакуации людей при пожаре и других ЧС из помещений учебного корпуса №10, пр. Ленина, 2 – 1 этаж.

В общественных зданиях и сооружениях на каждом этаже должно размещаться не менее двух переносных огнетушителей. Огнетушители следует располагать на видных местах вблизи от выходов из помещений на высоте не более 1,35 м. Размещение первичных средств пожаротушения в коридорах, переходах не должно препятствовать безопасной эвакуации людей.

Заключение

В данной работе поставлен вопрос о возможностях мультимодальной поведенческой статичной аутентификации в предопределенных пользовательских сценариях, которые недостаточно исследовались ранее. Спроектирована биометрическая система и разработана архитектура программного комплекса *ImplicitBio*, предоставляющего веб-приложениям сервис поведенческой аутентификации по статичным пользовательским сценариям. Детально описаны и разработаны ключевые модули системы *ImplicitBio* с использованием языка программирования *TypeScript* и нереляционной БД - *MongoDB*. Разработана и опубликована в Интернете исследовательская версия системы *ImplicitBio*, с помощью которой проведен двухнедельный эксперимент с участием 10 человек в ролях подлинных пользователей и злоумышленников, проходящих пользовательский сценарий «Форма логина». На основании эксперимента с помощью языка *R* проведен статистический анализ отклонений каждой биометрики для всех участников эксперимента и проведена корректировка состава и пороговой разности успеха биометрик поведенческого профиля. По данным первичного эксперимента рассчитаны параметры качества системы (FRR=6.15%, FAR=0%). Таким образом, предложенный в данной работе метод мультимодальной поведенческой аутентификации по статическим сценариям является эффективным и может быть использован в веб-приложениях в качестве дополнительной подсистемы аутентификации.

Список публикаций студента

1. А.Т. Газизов Система для исследования мультимодальной статичной поведенческой авторизации в веб-приложениях // II Всероссийская научно-техническая конференция с международным участием «Интеллектуальный анализ сигналов, данных и знаний: методы и средства» 11-13 декабря 2018, НГТУ, Новосибирск
2. А.Т. Газизов Модуль сбора пользовательских событий для исследования поведенческой авторизации в веб-приложениях // XVI Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии», 3-7 декабря 2018, ТПУ, Томск

Список использованных источников

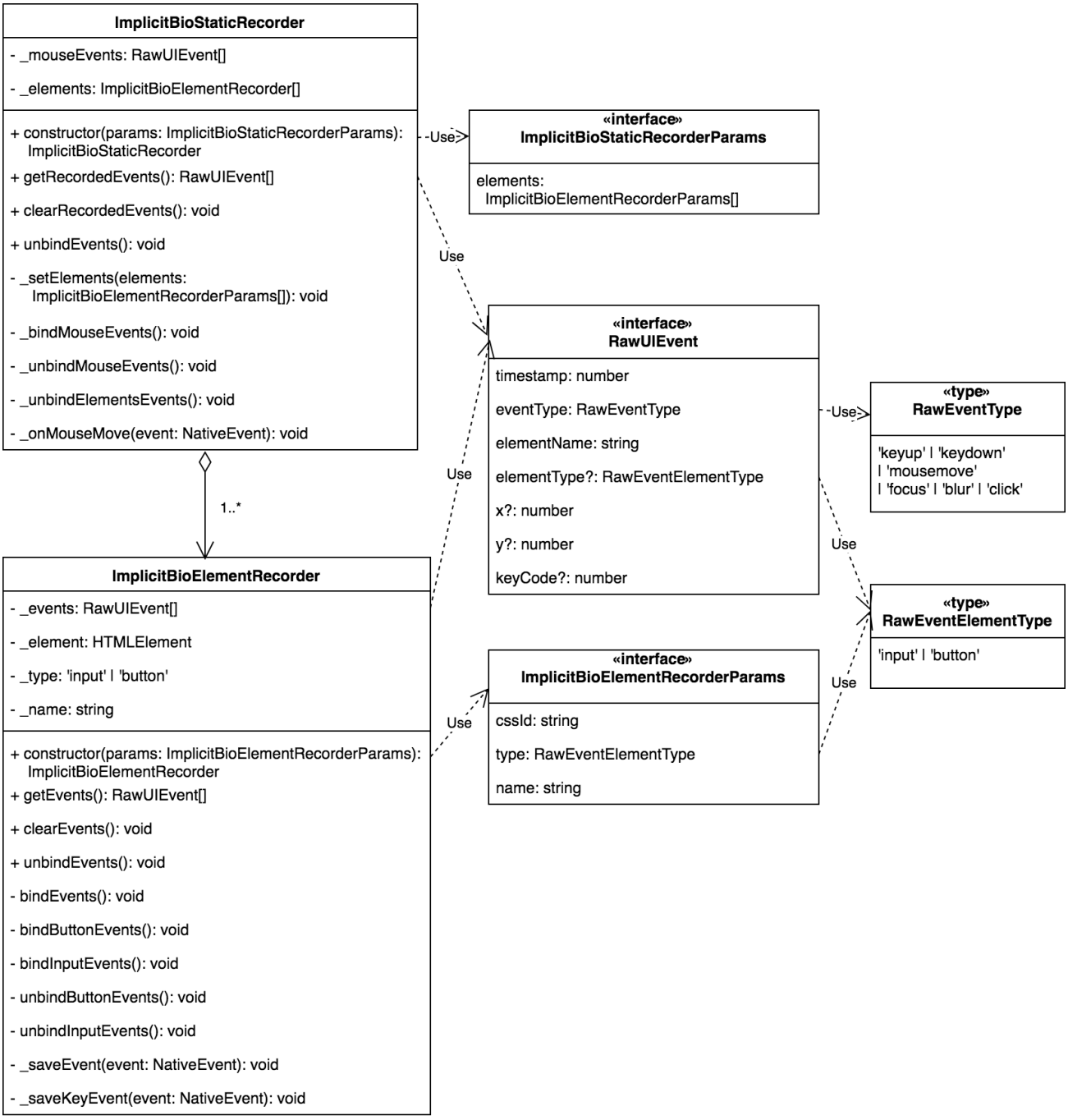
1. Bhattacharyya D, Ranjan R, Alisherov F, Choi M. Biometric authentic: a review. Int J Serv Sci Technol 2009; 2; 13-28.
2. V.M. Patel, R. Chellapa, D. Chandra and B. barbell, “Continuous User Authentication on Mobile Devices”, IEEE Signal processing magazine, vol. 33, no. 4, pp. 49–61, 2016.
3. H. Khan, U. Hengartner, and D. Vogel, “Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying”, in 11th Symp. Usable Privacy and Security (SOUPS 2015), 2015, pp. 225–239.
4. N. L. Clarke, Transparent User Authentication: Biometrics, RFID and Behavioural Profiling. London: Springer, 2011.
5. A.K. Jain, A. Ross and S.Prabhakar, “An introduction to biometric recognition”. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4-20, 2004
6. L. Wang, “Some issues of biometrics: Technology intelligence, progress and challenges,” International Journal of Information Technology and Management, pp.72 -82, 2012.
7. A. Dantcheva, C. Velardo, A. D’Angelo, and J. L. Dugelay, “Bag of soft biometrics for person identification. new trends and challenges,” Multimedia Tools and Applications, 51:pp. 739-777, 2011.
8. Joyce R, Gupta G. Identity authentication based on keystroke latencies. Commun ACM 1990;33:168-76.
9. Monrose F, Rubin A. Authentication via keystroke dynamics; 1997. pp. 48e56 [ACM Conference on Computer and Communications Security].
10. Bergadano F, Gunetti D, Picardi C. User authentication through keystroke dynamics. ACM Transactions Information Syst Secur 2002;5:367-97.
11. Marsters J. Keystroke dynamics as a biometric [Ph.D. thesis]. University of Southampton; 2009.
12. Gamboa H, Fred A. A behavioural biometric system based on human computer interaction. Proc SPIE, Biometric Technol Hum Identif 2004;5404:381e92
13. Pusara M. An examination of user behavior for user reauthentication [Ph.D. thesis]. Purdue University; 2007.
14. Shen C, Guan X, Cai J. A hypo-optimum feature selection strategy for mouse dynamics in continuous identity authentication and monitoring; 2010. pp. 349e53 [IEEE International Conference on Information Theory and Information Security].
15. Fehrer C, Elovici Y, Moskovitch R, Rokach L, Schclar A. User identity verification via mouse dynamics. Inf Sci 2012;201:19-36.
16. Issa Traore, et. all Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments // 2012 Fourth International Conference on Digital Home, 23-25 Nov. 2012
17. K. Bailey, J. Okolica, G. Peterson User identification and authentication using multi-modal behavioral biometrics // Computers & security, Vol. 43, June 2014, Pages 77-89
18. S. Mondal, P. Bours Combining keystroke and mouse dynamics for continuous user authentication and identification // 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)

19. Chao Shen et. al On the effectiveness and applicability of mouse dynamics biometric for static authentication: A benchmark study // 2012 5th IAPR International Conference on Biometrics (ICB), 29 March – 1 April 2012, New Delhi, India
20. Chao Shen et. al User Authentication Through Mouse Dynamics // IEEE Transactions on Information Forensics and Security, Volume: 8, Issue: 1, Jan. 2013, pp. 16–30
21. A. Ross, A. Jain Multimodal biometrics: An overview // 2004 12th European Signal Processing Conference, 6-10 Sept. 2004, Vienna, Austria.
22. Ahmed A, Traore I. Anomaly intrusion detection based on biometrics. In: IEEE Workshop on Information Assurance; 2005. pp. 1–7.
23. Pusara M. An examination of user behavior for user re-authentication [Ph.D. thesis]. Purdue University; 2007.
24. K.O. Bailey et al. User identification and authentication using multi-modal behavioral biometrics // Computers & Security, 43:77 – 89, 2014.
25. R. Gaines et al Authentication by Keystroke timing: some preliminary results // Tech Rep Rand Corp R-2526-NSF; 1980.
26. Joyce R, Gupta G. Identity authentication based on keystroke latencies. Commun ACM 1990;33:168-176.
27. Bleha S, Slivinsky B, Hussein B. Computer access security systems using keystroke dynamics // IEEE Transactions Pattern Analysis Mach Intell 1990;12:1217-22.
28. Brown M, Rogers S. User identification via keystroke characteristics of typed names using neural networks // Int J Man-Machine Stud 1993;39:999-1014.
29. Haider S, Abbas A, Zaidi A. A multi-technique approach for user identification through keystroke dynamics // IEEE Int Conf Syst Man Cybern 2000;2:1336-41.
30. Bartlow N. Evaluating the reliability of credential hardening through keystroke dynamics // Int Symposium Softw Reliab Eng 2006; 2006:117-26.
31. Hu J, Gingrich D, Sentosa A. A k-nearest neighbor approach to usr authentication through biometric keystroke dynamics // IEEE Conf Commun 2008; 2008:1556-60.
32. Pin Shen Teh et.al. A Survey of Keystroke Dynamics Biometrics. The Scientific World Journal 2013
33. A. A. E. Ahmed and I. Traore A new biometric technology based on mouse dynamics // IEEE Trans. Depend. Secure Comput., vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.
34. R. Everitt and P.W. McOwan. Java-Based Internet Biometric Authentication System // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(9): 1166-1172.
35. R. V. Yampolskiy and V. Govindaraju. Behavioral biometric: a survey and classification. International Journal of Biometrics, 2008, 1(1): 81-113.
36. S. Hashia, C. Pollett, and M. Stamp. On using mouse movements as a biometric // Proceeding of International Conference on Computer Science and its Applications, volume 1, 2005.
37. P. Bours and C. J. Fullu. A login system using mouse dynamics // Fifth International Conference of Intelligent Information Hiding and Multimedia Signal Processing, 2009:1072-1077.
38. H. Gamboa, A. L. N. Fred, and A. K. Jain. Web biometrics: user verification via web interaction // Biometrics Symposium, 2007:1-6.
39. K. Revett, H. Jahankhani, S. T. de Magalhes, and H. M. D. Santos. A survey of user authentication based on mouse dynamics // Proceedings of 4th International Conference on Global E-Security, pages 210-219, London, June 2008.

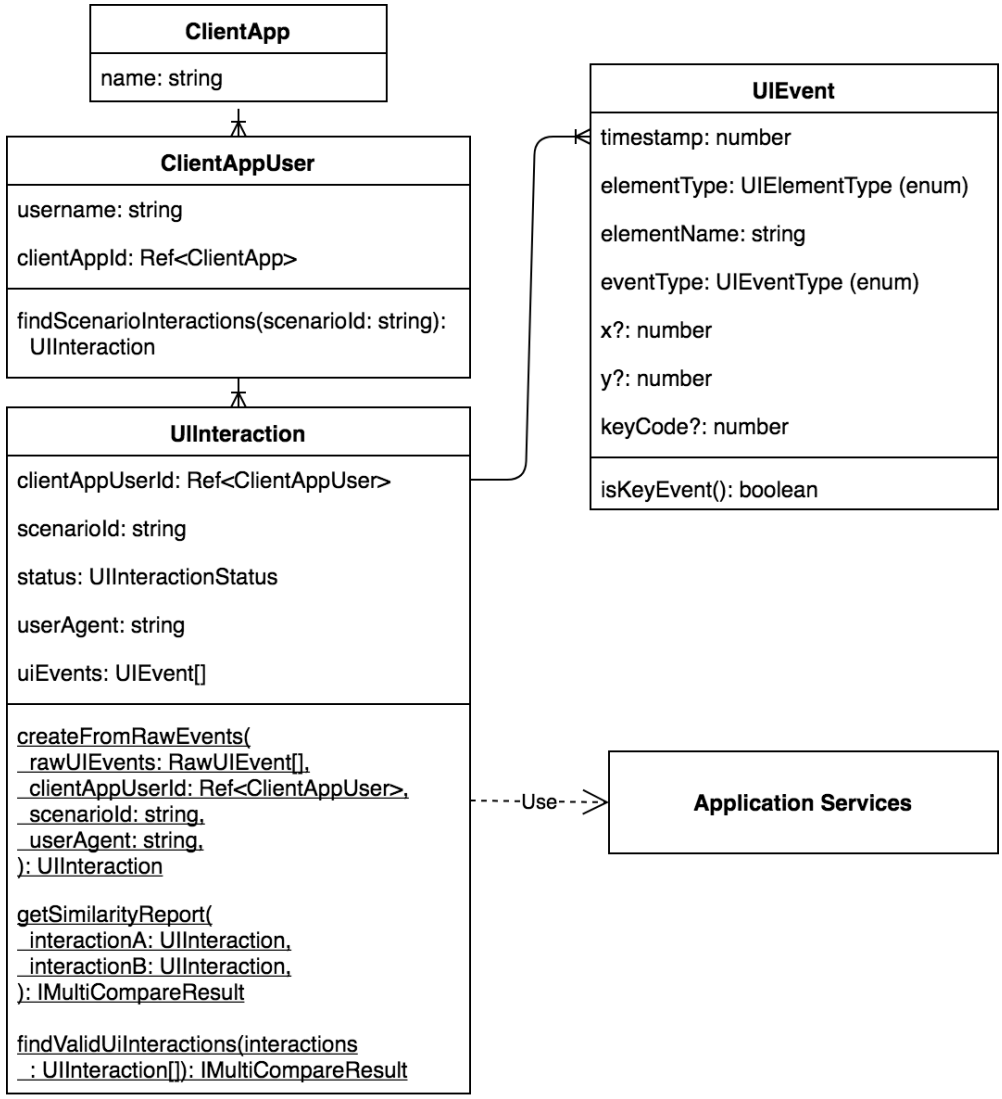
40. A. Ross and A. Jain, “Information Fusion in Biometrics,” // Journal of Pattern Recognition Letters, vol. 24, pp. 2115- 2125, 2003.
41. Mehdi Ghayoumi A review of multimodal biometric systems: Fusion methods and their applications // 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), 28 June-1 July 2015, Las Vegas, NV, USA
42. Node.js. URL: https://nodejs.org/en/ (Access date: 10.03.19).
43. DigitalOcean - Cloud Computing, Simplicity at Scale. URL: https://www.digitalocean.com/ (Access date: 10.03.19).
44. nginx. URL: https://nginx.org/ru/ (Access date: 10.03.19).
45. Bitbucket | The Git solution for professional teams. URL: https://bitbucket.org/product (Access date: 10.03.19).
46. MongoDB Hosting: Database-as-a-Service by mLab. URL: https://mlab.com/ (Access date: 10.03.19).
47. PM2 - Advanced Node.js process manager. URL: http://pm2.keymetrics.io/ (Access date: 10.03.19).
48. R: Box Plot Statistics. URL: https://stat.ethz.ch/R-manual/R-devel/library/grDevices/html/boxplot.stats.html (Access date: 10.03.19).
49. Keyboard biometrics – KeyTrac [Электронный ресурс]. – Режм доступа: https://www.keytrac.net/en - 24.03.2019
50. BehavioSec: Continuous Authentication Through Behavioral Biometrics –[Электронный ресурс]. – Режм доступа https://www.behaviosec.com - 24.03.2019
51. Н.А. Гаврикова и др. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение: учебно-методическое пособие / Н.А. Гаврикова, Л.Р. Тухватулина, И.Г. Видяев, Г.Н. Серикова, Н.В. Шаповалова; Томский политехнический университет. − Томск: Изд-во Томского политехнического университета, 2014. – 73 с.
52. СП 52.13330.2011 Свод правил. Естественное и искусственное освещение.
53. СанПиН 2.2.2/2.4.1340 – 03. Санитарно-эпидемиологические правила и нормативы «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». – М.: Госкомсанэпиднадзор, 2003.
54. СН 2.2.4/2.1.8.562 – 96. Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории застройки.
55. ГОСТ 12.1.038-82 ССБТ. Электробезопасность. Предельно допустимые уровни напряжений прикосновения и токов.
56. СанПиН 2.2.4.548 – 96. Гигиенические требования к микроклимату производственных помещений. М.: Минздрав России, 1997.
57. СанПиН П2.04.03-95 Нормы проектирования. Канализация. Наружные сети и сооружения
58. Охрана окружающей среды/Под ред. С.В.Белова. – М.: Высшая школа, 1991
59. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ.
60. НПБ 105-03. Нормы пожарной безопасности. Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности.
61. Технический регламент «о требованиях пожарной безопасности» [Электронный ресурс]: Единая справочная служба Консорциума «Кодекс». – Режим доступа: свободный. Ссылка доступа: http://ezproxy.ha.tpu.ru:2065/docs/

62. Безопасность жизнедеятельности. Учебник. Под ред. Э.А. Арустамова / 10-е изд., перераб. и доп. — М.: Изд-во «Дашков и К°», 2006. — 476 с.
63. СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий»
64. Назаренко, Ольга Брониславовна. Безопасность жизнедеятельности : учебное пособие / О. Б. Назаренко, Ю. А. Амелькович; Национальный исследовательский Томский политехнический университет (ТПУ). — 3-е изд., перераб. и доп. — Томск: Изд-во ТПУ, 2013. — 177 с.
65. СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование»
66. ГОСТ 17.4.3.04-85 «Охрана природы. Почвы. Общие требования к контролю и охране от загрязнения»

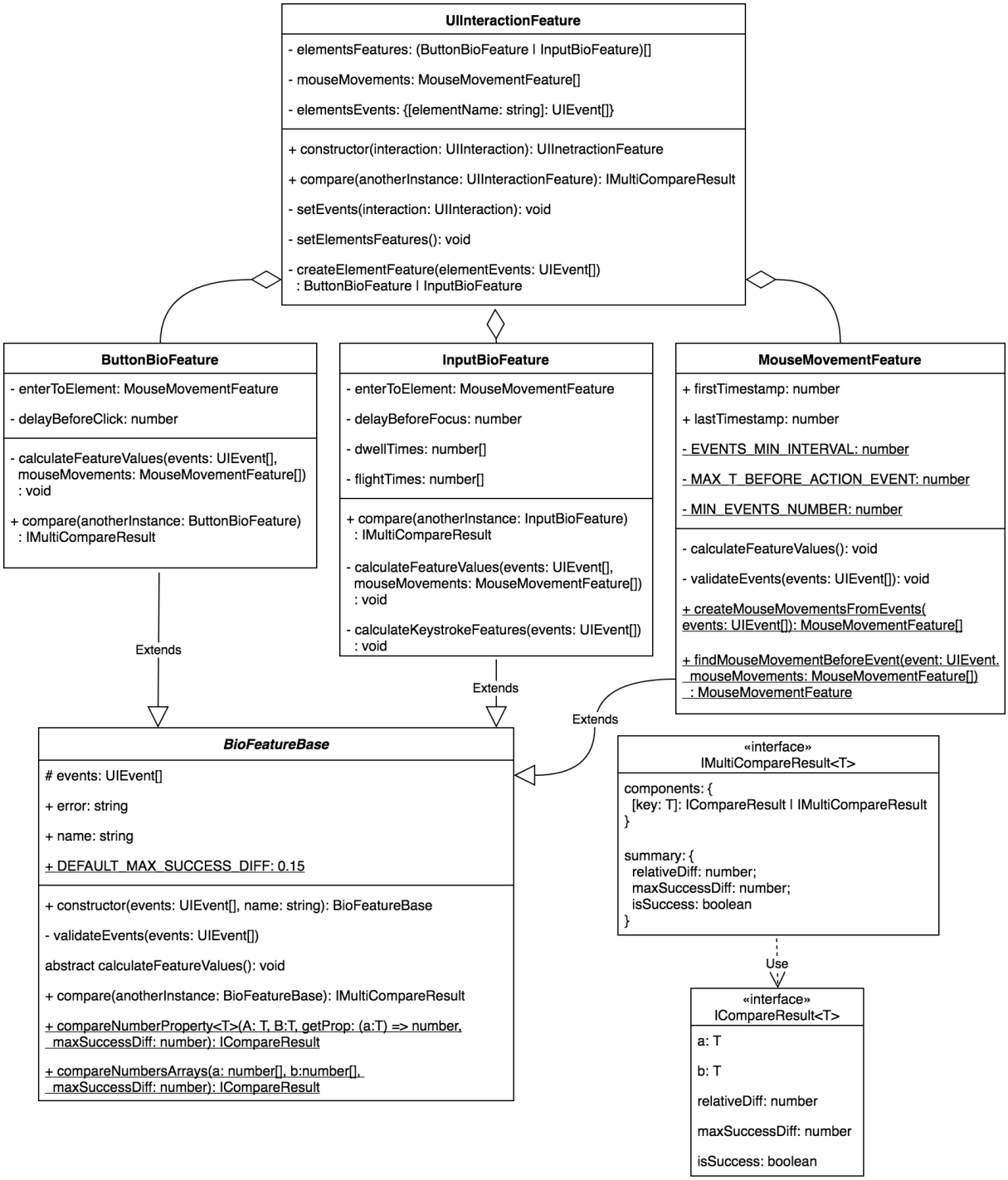
Приложение А. Диаграмма классов модуля ImplicitBio Recorder



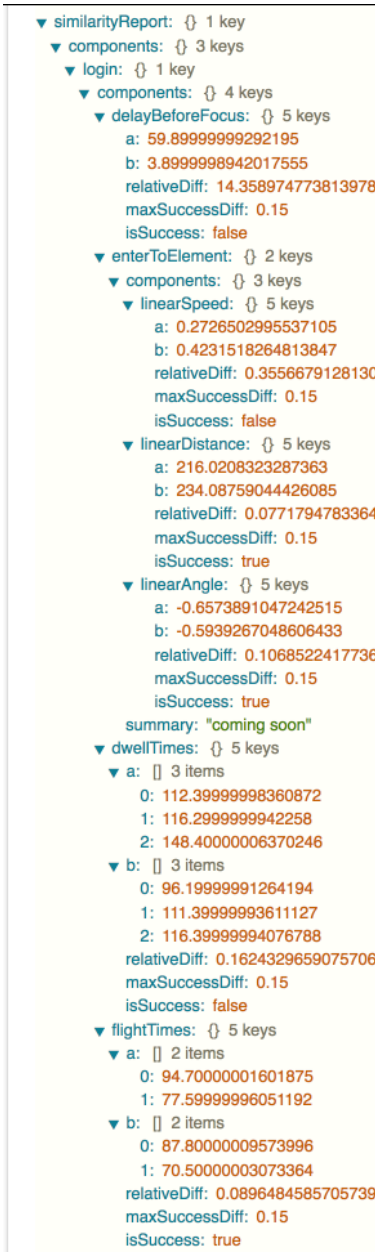
Приложение Б. Диаграмма классов моделей базы данных

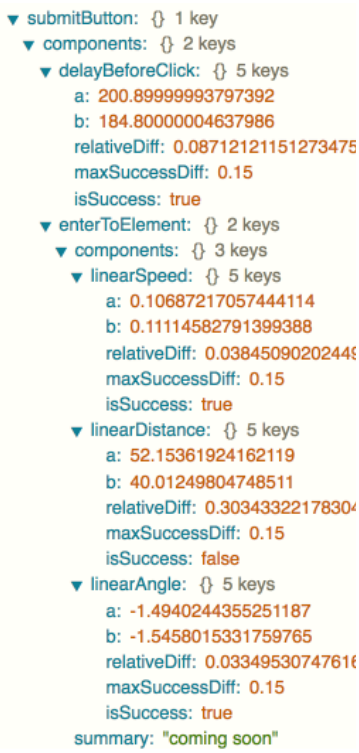


Приложение В. Диаграмма классов подмодуля *ApplicationServices*



Приложение Г. Результат мультимодального сравнения двух поведенческих профилей сценария заполнения формы авторизации

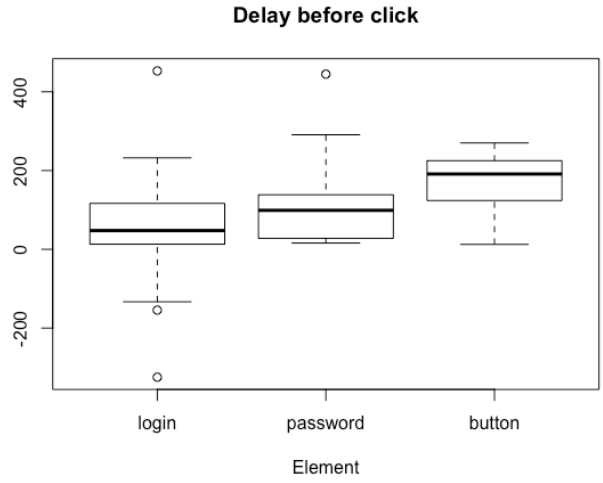


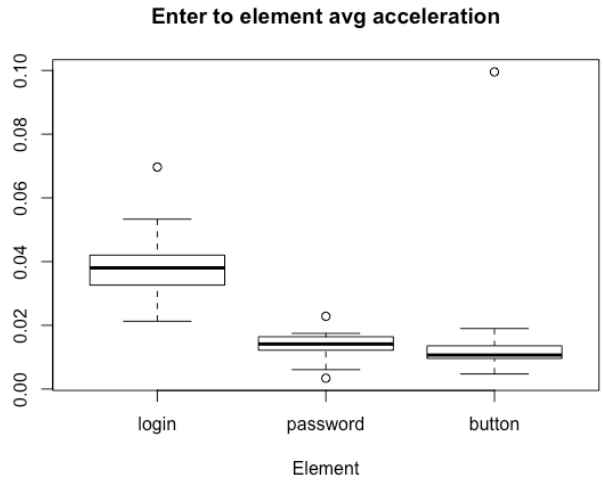


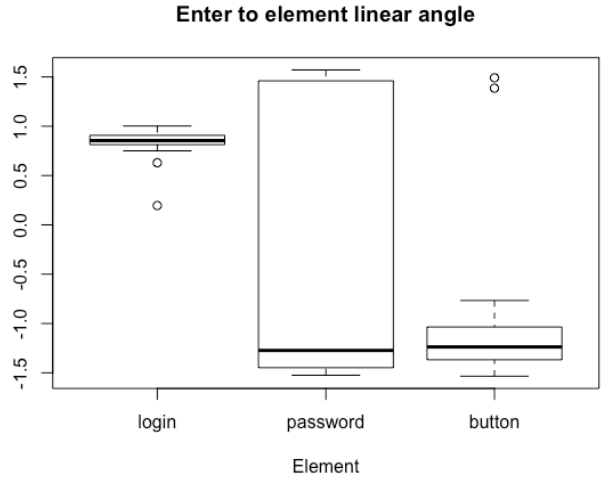
Приложение Е. Листинг для анализа данных многократного прохождения сценария «Форма логина» 1 пользователем.

```
library(jsonlite);
d <- fromJSON(
  "~/Documents/web/my/implicitauth/packages/implicitbio-server/dist/util/scripts/data/all.json",
  flatten=TRUE
);

# Common function to calculate each column relative variance (in %)
getRelativeVariances <- function(df) {
    result = c();
    for (colName in names(df)) {
      prepared <- df[, colName]
      vector <- na.omit(prepared[prepared > 0])
      relativeVariance <- (sd(vector)/mean(vector))*100;
      result <- c(result, relativeVariance)
    }
    result;
}

analyzeNumDf <- function(df, title) {
    boxplot(df, names=c("login", "password", "button"), main=title, xlab="Element")
    print('Relative variances')
    getRelativeVariances(df)
}

distances <- data.frame(
  d$components.login.enterToElement.linearDistance,
  d$components.password.enterToElement.linearDistance,
  d$components.submitButton.enterToElement.linearDistance
);
speeds <- data.frame(
  d$components.login.enterToElement.linearSpeed,
  d$components.password.enterToElement.linearSpeed,
  d$components.submitButton.enterToElement.linearSpeed
);
angles <- data.frame(
  d$components.login.enterToElement.linearAngle,
  d$components.password.enterToElement.linearAngle,
  d$components.submitButton.enterToElement.linearAngle
);
clicks <- data.frame(
  d$components.login.delayBeforeClick,
  d$components.password.delayBeforeClick,
  d$components.submitButton.delayBeforeClick
);

analyzeNumDf(clicks, "Delay before click")
analyzeNumDf(distances, "Enter to element linear distance")
analyzeNumDf(speeds, "Enter to element linear speed")
analyzeNumDf(angles, "Enter to element linear angle")

analyzeKeystrokeCol <- function(dfCol, title) {
  df_filered <- data.frame(do.call(rbind, dfCol))
  boxplot(df_filered, ylab="ms", xlab="Key", main=title)
  print('Relative variance')
  rvs <- getRelativeVariances(df_filered)
  mean(rvs)
}

analyzeKeystrokeCol(d$components.login.dwellTimes, 'login.dwellTimes');
analyzeKeystrokeCol(d$components.password.dwellTimes, 'password.dwellTimes');
analyzeKeystrokeCol(d$components.login.flightTimes, 'login.flightTimes');
analyzeKeystrokeCol(d$components.password.flightTimes, 'password.flightTimes');
```

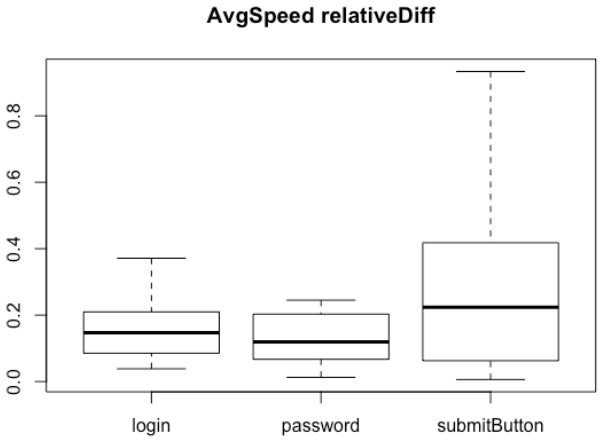
Приложение Ж. Диаграммы размахов значений метрик по данным многократного прохождения сценария «Форма логина» пользователем *User1*.

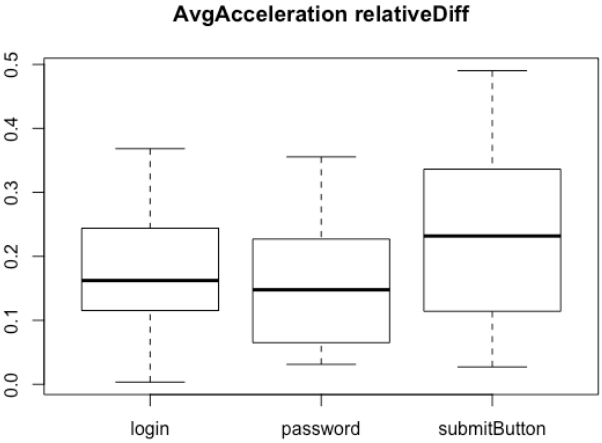


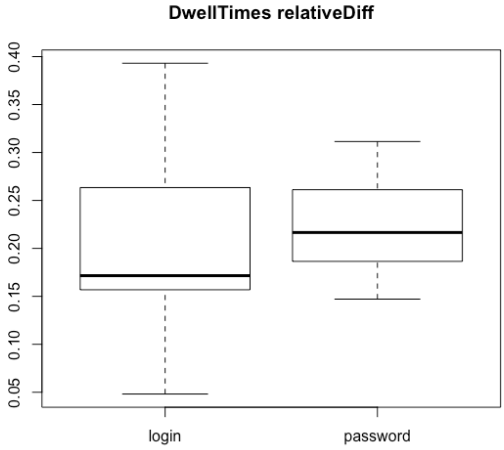


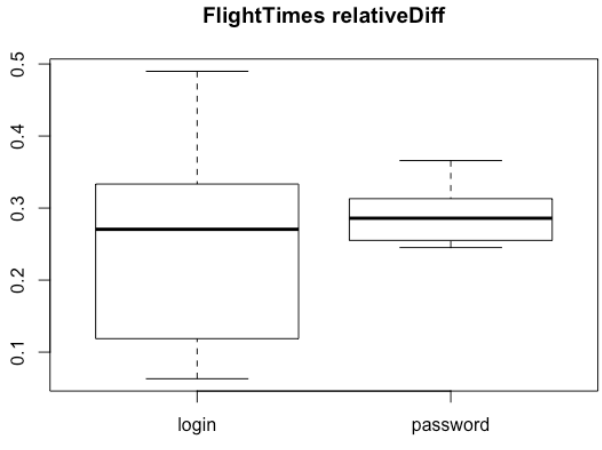


Приложение 3. Диаграммы размахов относительной разности метрик между последовательными прохождениями сценария «Форма логина» для 10 пользователей.









Приложение Е

Chapter 1
Biometric System Design

Студент:

Группа	ФИО	Подпись	Дата
8ПМ7И	Газизов Александр Тальгатович		

Консультант ОИТ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ	Соколова Вероника Валерьевна	к.т.н		

Консультант – лингвист отделения ОИЯ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИЯ	Диденко Анастасия Владимировна	к.ф.н.		

1. Biometric System design

Behavioural biometrics such as keystroke and mouse dynamics have been considered as means to perform authentication for several decades [1]. Though there is a lot of research in both of these techniques, there has been less work done on combining these two methods into one system for static authentication by particular user scenarios in web environment. This work considers the fusing of keystroke and mouse dynamics of different UI-elements bounded to particular user scenarios in web-applications.

1.1. Keystroke dynamics

Gaines et. al [1] introduced the idea of using behavioural biometrics as a supplement to traditional authentication. Initially, keystroke timing data was used to supplement password entry [2-4]. This evolved into the ability to analyse a long-structured text as a basis for authentication [5, 6], and, finally, long free text samples [7, 8]. Although the long free text better imitates free use, interest in keystroke timing to supplement password entry has remained [9, 10]. Each paper uses a similar set of features for classification. Research has been done using several statistical classifiers that has gotten similar results in terms of classification accuracy [11].

Generally, raw keystroke data is collected via registering user's events, such as 'key down' and 'keyup' events. By performing simple mathematical operation to timestamps deriving from raw keystroke data, timing duration or interval between consecutive keystrokes can be obtained. Timing information of two consecutive keystrokes, better known as *di-graph*, is the major feature data represented in keystroke dynamics domain [12]. It is widely categorized into two types, namely, *Dwell Time* and *Flight Time* (Figure 1).

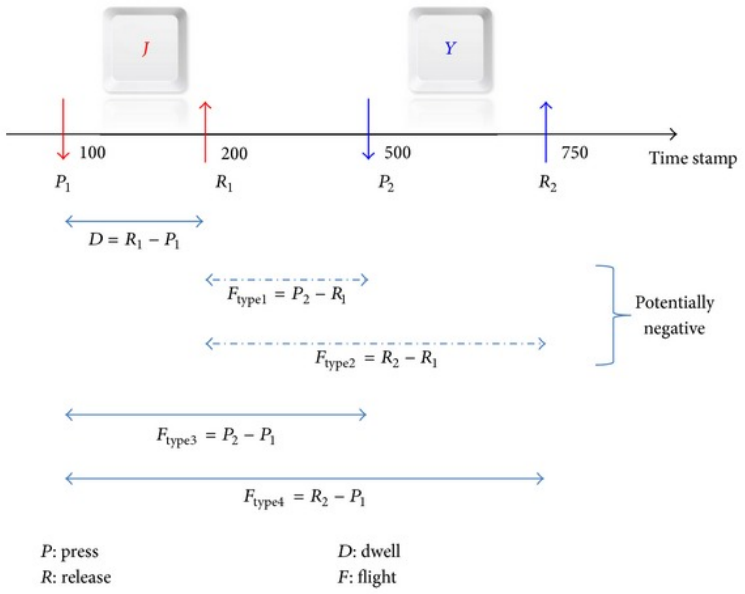


Figure 1. Different keystroke events of two characters "*J*" and "*Y*" with the formation of dwell time and flight time.

Dwell time (DT) refers to the amount of time between pressing and releasing a single key, in other words, how long a key was held pressing down. DT can be calculated by

$$\mathrm{DT}_n = R_n - P_n,$$

where *R* and *P* indicate the time stamp of release and press of a character, respectively, while *n* indicates the position of the intended DT. The number of DT generated will always be the same as the length of a given string.

Flight time (FT) refers to the amount of time between pressing and releasing two successive keys. It always involves key event (press or release) from two keys. FT may exist in four different forms as depicted in Figure 1. The formulas to calculate each form are listed as follows:

$$\mathrm{FT}_{\mathrm{type1},n} = \mathrm{P}_{n+1} - \mathrm{R}_n,$$
$$\mathrm{FT}_{\mathrm{type2},n} = \mathrm{R}_{n+1} - \mathrm{R}_n,$$
$$\mathrm{FT}_{\mathrm{type3},n} = \mathrm{P}_{n+1} - \mathrm{P}_n,$$
$$\mathrm{FT}_{\mathrm{type4},n} = \mathrm{R}_{n+1} - \mathrm{P}_n,$$

where *R* and *P* indicate the time stamp of release and press of a character, respectively, while *n* indicates the position of the intended FT. Differing from DT, the number of FT generated will always be one less than the length of a given string. Each type of FT gives

similar information about keystroke and there is no known information about what metric is better.

N-graph refers to the timing measurement between three or more consecutive keystroke events. It is better known as the elapse time between a key and the *n*th key event of a typing string. Despite many combinations of elapse time (ET), it can be extracted; the equation below is the most widely used when *n*-graph is concerned [13]. The following formula is considered:

$$ET_k = P_{k+n} - P_k,$$

where *P* indicates the time stamp of pressing a character, *n* denotes *n*th number of graphs employed, while *k* represents position of the intended elapse time. The total number of timing vector of ET exists in *n*-graph which can be seen as follows:

$$V_{ET} = \{ET_1, ET_2, ET_3, \ldots, ET_{s-n+1}\},$$

where *s* denotes the summation of characters in a typing sequence.

In [14], authors notice that 80% of research papers used *di-graph*; 7% used *tri-graph*; only 4% used *n*-graph. The ability to generate significantly more instances of timing vectors could be the reason for the popularity of *di-graph*. As a result, any value of *n* that is greater than 3 (tri-graph) was rarely chosen except for the experiment that involved huge amount of input text. Thus, in this work we will use the most common keystroke features that are *Flight* and *Dwell* times.

1.2. Mouse dynamics

Interest in mouse dynamics has been growing [15-16]. Current applications of mouse dynamics approaches could be classified into two classes, static authentication and continuous authentication [17]. The static authentication approaches analyse a user's mouse behaviour at some particular moments, e.g. login time. They usually require the user to perform a certain sequence of mouse operations, and compare the extracted features with a legitimate user's profile to check the user's identity. In this section, we review current methods for static authentication using mouse dynamics. When Everitt [18] first time researched if users could be distinguished by their mouse dynamics, several methods for static authentication based on mouse dynamics biometric have been proposed [20-24].

Gamboa et al. [20] described an authentication system for web-application based on mouse movements while the user inputs the PIN number. In the suggested approach, the system showed an on-screen virtual keyboard and requested users to only use mouse to enter the username-password pair. They reported an equal error rate of 6.2% based on 15 mouse strokes data for experiments on data from 50 users.

Aksari et al. [21] described continuous static authentication system for user's verification based on their mouse movements. Mouse features were extracted from 9 movements. They reported an equal error rate of 5.9% for 10 users.

Hashia et al. [22] described login scheme using a two-phased approach and mouse movements, in which both registration and authentication phases include moving the mouse pointer between pairs of dots shown consecutively on the screen. They collected data from 15 students in controlled environment and reported equal-error rate for this approach was 15%, with authentication time of 20 seconds.

Revett et al. [23] described static authentication system based on mouse dynamics where a user was authenticated by interacting with a graphical GUI interface featuring icons arranged on a circular dial. They reported an average false acceptance rate (FAR) and false rejection rate (FRR) of around 3.5% and 4% respectively in a small-scale evaluation including 6 persons.

Bours et al. [24] presented an authentication method based on mouse movements in uncontrolled environment, including 28 participants. In their study participants were asked to play a task given the pre-defined path. They reported an equal-error rate of 26.8% for experiments with 28 persons.

Table 1. Mouse features used in static mouse dynamics authentication [20]

Mouse Features	**Definitions**
Travelled distance	The distance between two adjacent position of mouse click actions.
Movement offset	The distance between the practical mouse trajectory and the ideal mouse trajectory.
Movement elapsed time	The time interval between a starting point and an ending point of mouse movements.
x-speed	The movement speed in abscissa direction.
y-speed	The movement speed in ordinate direction.
x-speed against distance	The movement speed compared to travelled distance in abscissa direction.

y-speed against distance	The movement speed compared to travelled distance in ordinate direction.
Average speed against distance	Average movement speed compared to accumulative travelled distance.
x-acceleration	The movement acceleration in abscissa direction.
y-acceleration	The movement acceleration in ordinate direction.
x-acceleration against distance	The movement acceleration compared to travelled distance in abscissa direction
y-acceleration against distance	The movement acceleration compared to travelled distance in ordinate direction
Acceleration against distance	Average movement acceleration compared to accumulative travelled distance.

In this work, we consider static authentication for fixed user scenarios, and use the following mouse dynamics features: *delayBeforeClick*, *linearAngle*, *avgSpeed*, *avgAcceleration*. These features were chosen because of their efficiency and ease of implementation.

1.3. Multimodal biometric systems

Unimodal biometric systems are known for their good performance and efficient identification [25], but they have several problems:

1. Noise in sensed data: variations and noise in biometric information might make false matches in the database.

2. Non-universality: there can be exceptions when a person is not able to provide a particular biometric.

3. Intra-class variation: the biometric data acquired during authentication can be different from the data used for registration.

4. Inter-class similarities: it means the overlap of features corresponding to multiple persons.

5. Spoof attacks: unimodal systems are vulnerable to spoof attacks.

Besides, the performance of unimodal systems is seriously dependent on the conditions of the users' illumination, health, type of sensor, etc. [9-10]. Multimodal systems are able to overcome most of the above weaknesses and attract the attention of many researchers in different disciplines [9–12]. Its performance is superior to unimodal biometric systems, they have higher accuracy, noise resistance, universality, anti-spoofing attacks, and more robust

than unimodal ones. The best solution to solve these problems is creating multimodal systems which are based on multiple sources of information.

A multimodal biometric system becomes increasingly common in current and future real-world biometric system deployment. These are some advantages of these systems:

1. Recognition accuracy: the most immediate advantage of a multimodal biometric system is recognition accuracy.

2. Biometric data enrolment: multimodal biometric systems can address the problem of non-universality.

3. Privacy: multimodal biometric systems increase resistance to certain type of vulnerabilities.

Several researchers have attempted to combine multiple forms of biometric based authentication to improve the accuracy of the overall system. Asha and Chaliapin [26] combined fingerprint biometrics with mouse dynamics in order to identify the users enrolled in the e-learning class. Rabuzin et al. [27] also made the case that combined multiple biometric techniques which would be beneficial in creating a more robust authentication method for e-learning platforms. Other combinations include voice and facial recognition, facial recognition and a fingerprint, voice, facial recognition and a fingerprint; iris and retinal features.

Ahmed and Traore [28] integrated keyboard and mouse dynamics into a single architecture that could act as an intrusion detection system. Twenty-two people were asked to install a monitoring system on their workstations that collected keystrokes and mouse information. They ran the software for nine weeks. A neural network was created and trained for each user. Doing this for all 22 users Ahmed et al. were able to achieve a FAR of 0.651% and a FRR of 1.312%.

Pusara [29] integrated keyboard, mouse dynamics and graphical user interface information into the integrated architecture that could also act as an intrusion detection system. Pusara enlisted 61 volunteers from undergraduate and graduate students to use a Windows machine and behave normally as they reviewed a reading assignment and then answered a set of twenty questions. They had ten days to complete the assignment and some of them worked on it over multiple days. Pusara calculated latencies and durations for digraphs as well as the mean, standard deviation and skewness as well as the number of occurrences of each alphabet

letter and numeral. For mouse events, Pusara calculated the number of mouse movements as well as the mean, standard deviation, and skewness of distance, speed, angle of orientation, X-coordinates, Y-coordinates, and duration between movements. Finally, Pusara collected spatial and temporal GUI events that included items like minimizing, maximizing, restoring, moving windows, opening and closing processes, and selecting menus and buttons. Pusara then performed some smoothing to improve the results. The final results were a FAR 23.37% and a FRR of 1.50%.

Bailey et. all [30] presented a behavioural biometric system that fused user data from a keyboard, a mouse, and Graphical User Interface (GUI) interactions. They tested the system over 31 users and showed that fusion techniques significantly improved behavioural biometric authentication accuracy over single modalities on their own. They achieved a FAR of 2.10% and a FRR of 2.24%.

The majority of the papers, related to behaviour multimodal biometrics, studies continuous authentication. Despite universality of such systems, they require some amount of time or actions to make a decision. Besides, they do not consider that keystroke and mouse metrics can be dependent on the particular task done by user: e.g. whether the user moves the mouse to a button or to an input; even the type of a button (“cancel” or “submit”) can make metrics different. Static authentication for fixed user scenarios can consider such factors and can be applied immediately when the scenario finishes. However, known papers for static authentication are applicable only for one scenario (e.g. login form). In this work, we consider a static multimodal behavioral biometrics system for arbitrary fixed user scenarios bounded to GUI elements.

1.4. Modalities fusion

A fusion of biometric modalities can occur in different ways. According to Ross and Jain [31], in biometric systems a fusion can occur by fusing features together, fusing matching scores together, or a fusion of the decisions made by each individual modality.

In the feature level fusion (Figure 2), signals are first processed and feature vectors are extracted separately from each biometric trait. After that, these feature vectors are combined to form a composite feature vector which is further used for classification. Since features

contain richer information of a biometric trait than a matching score or a decision of matcher, a fusion at feature level is expected to provide better recognition results, but it has also been observed that when features of different modalities are compatible with each other, fusion at feature level achieves more accuracy [32].

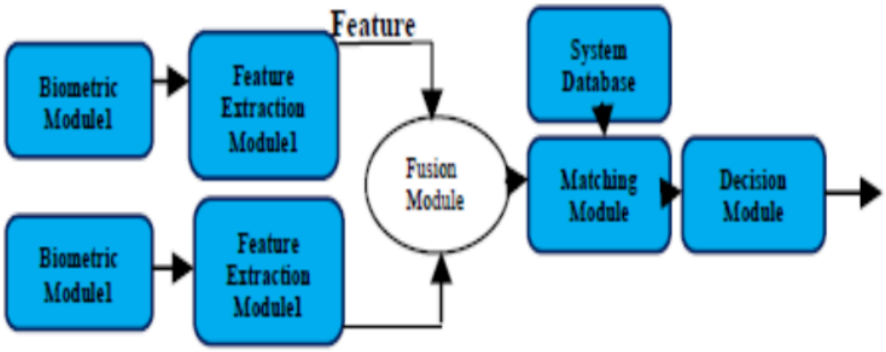


Figure 2. Feature level fusion [32]

In this matching score level fusion, feature vectors are processed separately instead of being combined and a matching score is found individually. Finally, these matching scores are combined to make classification. Various statistical learning techniques may be used to combine match scores. A match score-level fusion is also called confidence-level fusion.

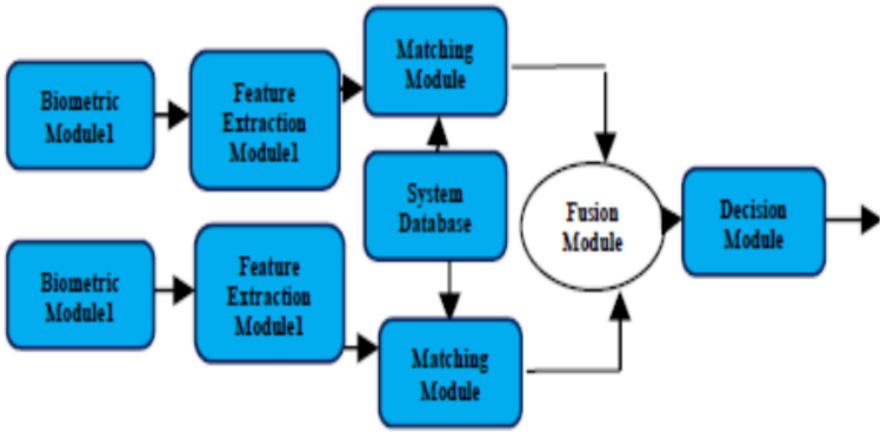


Figure 3. Matching score level fusion [32]

In decision level fusion, each modality is first pre-classified independently, i.e. each biometric trait is captured, then features are extracted from that captured trait, based on these extracted features. Final classification is based on the fusion of the outputs of different modalities. This is the highest level of a fusion with respect to a human interface. In other words, the decision from each biometric system is concluded to make the final decision. In this work, we use the decision level fusion to obtain the final result of authentication.

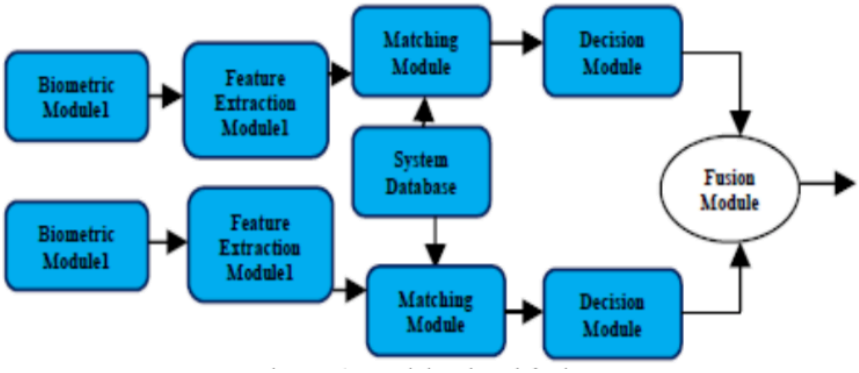


Figure 4. Decision level fusion [32]

1.5. Existing web services for behavioural authentication

Increasing demand for novel authentication methods in web-applications leads to the emergence of commercial web services offering the behavioural-based authentication layer for other applications. In general, an operation scheme of such services is similar: a service provides a client-side library that is included in the web-application page and is configured with parameters for a user identification and, in case of static authentication, for identification of GUI elements on the page. The client-side library records user events and calculates a behavioural biometrics profile which is then sent directly or via application backend to the service backend which responds with the result of authentication. In what follows, we briefly overview the most popular existing web-services providing behavioural authentication for web-applications.

Key Track [33] is a web-service providing only keystroke authentication. Their client-side library records a relative dwell, flight time and a key code of each key while a user is typing in a textbox. The system can operate in two modes: “password hardening” and “any text”. The “password hardening” operation mode is intended to be used for enhancing the security of password based authentication. By using this feature, one can add a static biometrics-based security layer to an application. The “any text” operation mode is suitable for identifying users based on the keystroke dynamics while typing arbitrary text phrases.

Another example of keystroke-only authentication service is TypingDNA [34]. They propose to use keystroke-based authentication instead of common two-factor authentication methods, such as SMS or voice verification. Their demo shows a login form and a credit card

payment form. Beside common API for authentication in web-applications, they also have an extension for Chrome browser which allows passing two-factor authentication without a phone.

Biocatch company [35] provides a service for continuous behavioural authentication. Their technology is based on so called “Invisible Challenges”: patented techniques that introduce subtle tests into the online session that users subconsciously respond to without sensing any change in their experience. They use more than 2000 behavioural parameters of user-device interactions to generate real-time risk scores based on a wide range of human and non-human cybersecurity threats. The company proposes to use their service for identity proofing, continuous authentication, account takeover fraud and vishing scams.

Behaves [36] is another service for continuous risk based authentication. They provide a platform that easily integrates with web and mobile apps to combat account related fraud by the means of continuous behavioural biometrics including keystroke and mouse dynamics analysis. BehavioSec describes several case studies of their service application: remote access continuous authentication; removing bots and reducing new account fraud; protecting financial transactions; verifying digital identities beyond one time passwords and protecting SaaS revenue.

All the existing known web services for behavioural authentication provide either single modality static authentication (e.g. KeyTrack, TypingDNA) or continuous multimodal authentication (e.g. BioCatch, BehavioSec). In this work, we consider development of the web-service for multimodal static authentication.